Siber International Journal of Advanced Law (SIJAL)
E-ISSN : 2987-5595
P-ISSN : 2987-5609
https://review.e-siber.org/SIJAL siberpublisher.info@gmail.com +62 812-1046-7572
DOI: https://doi.org/10.38035/sijal.v4i2.474
https://creativecommons.org/licenses/by/4.0/
Received: 04-11-2026 | **Revised:** 18-11-2026 | **Accepted:** 21-11-2026

The Legal Liability of Online Lending Service Providers for the Misuse of Users' Personal Data

Sascha Kezia Cenniago[1], Vanessa Maurent[2], Beatrice Callista Yo[3], Stephanie Sigrid[4], Owen Edgar Kuncoro[5], Pietro Grassio Ekoyulio[6]
[1]Universitas Pelita Harapan, Banten, Indonesia, keziacenniago@gmail.com
[2]Universitas Pelita Harapan, Banten, Indonesia, vanessamaurent0610@gmail.com
[3]Universitas Pelita Harapan, Banten, Indonesia, beatricecallistayo@gmail.com
[4]Universitas Pelita Harapan, Banten, Indonesia, stephaniesigrid@gmail.com
[5]Universitas Pelita Harapan, Banten, Indonesia, kuncoroowen@gmail.com
[6]Universitas Pelita Harapan, Banten, Indonesia, pietro.ekoyulio@lecturer.uph.edu

Corresponding Author: stephaniesigrid@gmail.com[4]

Abstract: The development of online lending services, or Information Technology-Based Joint Funding Services, has facilitated access to financing while increasing the risk of personal data misuse. Service providers collect and process personal data from user identification to debt collection, requiring adequate data protection mechanisms. This study aims to examine personal data protection regulations, forms of data misuse, the legal liability of service providers, and legal remedies available to affected users. This research employs a normative legal method with statutory and case approaches. The analysis is based on Law Number 27 of 2022 concerning Personal Data Protection, Financial Services Authority Regulation Number 40 of 2024, and Central Jakarta District Court Decision Number 597/Pid.Sus/2021/PN.Jkt.Pst. The findings indicate that service providers, as Personal Data Controllers, are obligated to maintain data confidentiality and security and prevent unauthorized access. Misuse may involve internal or external parties, including fictitious debt collection and disclosure of personal information. Service providers may incur administrative, criminal, and civil liability, subject to the elements of fault and causation. Therefore, legal protection requires law enforcement, preventive measures, and effective data security governance by online lending service providers.

Keywords: Online Lending, Personal Data, Legal Liability, Personal Data Protection.

INTRODUCTION

The development of financial technology has transformed the way society interacts and conducts payment transactions. One of the increasingly prominent and rapidly developing financial technology services is Information Technology-Based Joint Funding Services

("**LPBBTI**"), commonly known as online lending or financial technology ("**fintech**"). These lending services utilize digital applications to facilitate access to financing, particularly for individuals who may not be served by conventional financial institutions. Alongside these developments, digital interaction has increased significantly, involving the extensive collection, storage, and processing of consumers' personal data. Within the fintech business model, personal data plays a crucial role throughout various stages, ranging from the identification and verification of prospective borrowers, creditworthiness assessments, and transaction monitoring to debt collection activities (Anggraini & Wiraguna, 2025).

As of December 31, 2024, there were 97 licensed fintech lending providers. Meanwhile, in January 2025, financing within the fintech peer-to-peer lending industry reached IDR 78.50 trillion, reflecting continued annual growth. During the same period, the Financial Services Authority ("OJK") received 4,472 complaints through its Consumer Protection Portal application, of which 1,643 originated from the fintech industry. These figures indicate that consumer protection in the sector remains inadequate. Given that financing services have facilitated economic activities amounting to tens of trillions of rupiah, there is an increasing need for sound business governance that prioritizes personal data security and user protection. Furthermore, personal data may cause harm to data subjects when processed beyond legally permissible purposes.

Research indicates that the development of online lending has expanded access to credit while simultaneously creating problems involving the disclosure of personal data and its improper use. These disruptive effects may generate instability within the financial sector and encourage unhealthy competition, particularly due to the ease of obtaining loans. Risks may also arise from internal parties who possess legitimate access but subsequently exploit such access for unauthorized purposes. In this regard, Law Number 27 of 2022 concerning Personal Data Protection ("PDP Law") clarifies the legal position of Personal Data Controllers. Data Controllers are obligated to protect and ensure the security of processed personal data, maintain its confidentiality, supervise every party involved in data processing, prevent unlawful processing, and safeguard personal data against unauthorized access (Priliasari, 2019).

The Central Jakarta District Court Decision Number 597/Pid.Sus/2021/PN.Jkt.Pst provides a concrete example of this legal issue. The case illustrates how user data obtained through an employment relationship may remain under an individual's possession even after the employment relationship has ended. In this case, Michael Lisardo had previously worked in the debt collection departments of fintech companies PT Malkom Burung Indonesia and PT Zeus Indonesia. After leaving his employment, he continued to retain customer data belonging to both companies in the form of telephone contacts. Michael subsequently used this information to conduct fraudulent debt collection activities. On May 14, 2021, the defendants engaged in fraudulent collection activities targeting approximately 30 customers through WhatsApp messages. They offered payment discounts and threatened to publicly expose the customers' personal information by creating a WhatsApp group named "*KORBAN/NASABAH MALING PUNYA UTANG GA BAYAR*" (Victims/Customers Who Steal by Failing to Pay Their Debts). One of the victims, Krismawati Ubaeni, was instructed to transfer IDR 2,000,000 through a virtual account. However, the payment did not reduce her outstanding loan obligations within the lending application, as the money was instead transferred directly to the defendants.

From the perspective of criminal liability, the court found Michael Lisardo and Sunandar legally and conclusively guilty of committing a criminal offense under Article 28 paragraph (1) in conjunction with Article 45 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions ("**ITE Law**"), the offense involved the dissemination of false and misleading information resulting in consumer losses in electronic transactions. Both defendants were

sentenced to one year of imprisonment and a fine of IDR 1 billion each. However, PT Malkom Burung Indonesia and PT Zeus Indonesia were not subjected to any criminal sanctions.

This decision establishes a factual connection between the customers and the service providers' former employees but does not examine whether the companies had implemented adequate measures to protect the personal data in their possession. The court did not assess the companies' potential negligence in revoking access rights, controlling retained copies of personal data, or supervising the use of such data within the framework of corporate accountability. Research further indicates that fintech data controllers are the parties responsible for establishing lawful grounds for data processing and ensuring the protection of personal data (Hanifawati, 2021).

Under the PDP Law, the central issue lies in determining which party has the capacity to control and mitigate the risks before the misuse occurred. If service providers determine the purposes of processing, grant access to personal data, and manage the relevant systems, liability cannot logically be attributed exclusively to one party.

Furthermore, Article 37 of the PDP Law requires Personal Data Controllers to supervise every party involved in processing activities under their control. Article 39 requires Data Controllers to prevent unauthorized access to personal data. The obligations demonstrate that the law does not wait until personal data has been misused before imposing legal responsibilities. Rather, preventive obligations arise from the moment data processing activities commence. In the context of LPBBTI providers, these preventive obligations may be implemented through access control mechanisms, authentication systems, activity logging, supervision of internal and external parties, and appropriate measures following the termination of employment relationships. Accordingly, the legal liability LPBBTI provides must be examined through several interconnected legal frameworks.

From an administrative law perspective, violations of data security and governance obligations may result in regulatory sanctions. POJK 40/2024 provides OJK with the authority to impose administrative sanctions for violations of obligations concerning electronic systems. Meanwhile, the PDP Law establishes mechanisms for administrative and criminal sanctions against certain violations. From a civil law perspective, losses resulting from unlawful personal data processing may also constitute grounds for claims for damages, provided that the elements of civil liability are fulfilled.

This issue highlights the urgency of the present research, considering that the fintech industry will continue to expand while personal data remains an integral component of its business operations. At the same time, cases involving data breaches and personal data misuse in Indonesia demonstrate that data security risks are not merely hypothetical. If the law only provides remedies after an individual has misused personal data, the preventive function of Data Controllers' obligations will not operate optimally. Conversely, imposing liability on service providers without establishing clear parameters concerning fault and causation may result in an excessively broad scope of liability.

Based on the foregoing background, this research formulates the following research questions;

1. How is the protection of users' personal data in online lending services regulated under the applicable laws and regulation in Indonesia?
2. What are the forms and patterns of personal data misuse involving users of online lending services in Indonesia?
3. What form of legal liability may be imposed on online lending service providers for the misuse of users' personal data, and what legal remedies are available to affected users?

METHODS

This research uses a normative legal research method with a prescriptive-analytical approach. It focuses on analyzing legal provisions governing personal data protection in the operation of LPBBTI, as well as examining the legal responsibility of service providers for the misuse of users' personal data. The research is designed to address three main issues: the regulation of personal data protection, the forms of personal data misuse in online lending services, and the legal responsibility of service providers, including the legal remedies available to affected users.

This research applies two approaches: the statutory approach and the case approach. The statutory approach is carried out by identifying, reviewing, and interpreting relevant legal provisions, particularly the PDP Law and POJK 40/2024, along with other regulations related to consumer protection and electronic system providers. The analysis focuses on the relationship between data controllers' obligations, the principles of lawful personal data processing, supervision requirements, the prevention of unauthorized access, and legal accountability mechanisms. The case approach examines Central Jakarta District Court Decision Number 597/Pid.Sus/2021/PN.Jkt.Pst. The analysis covers the relevant legal facts, the actions considered by the court, the legal provisions applied, and the scope of responsibility of the parties convicted in the case. The findings are then compared with the preventive obligations of service providers as Personal Data Controllers under the relevant regulations. This comparison aims to assess whether the issue of controlling data access after the end of an employment relationship was addressed in the court's considerations or still requires further legal analysis.

The legal materials used in this research consist of primary legal materials, including legislation and court decisions, as well as secondary legal materials, such as relevant books and academic journal articles. The materials are collected through library research based on the three main research focuses: regulation, forms of misuse, and legal responsibility. The analysis is conducted qualitatively through the classification of legal materials, interpretation of legal provisions, and their application to the facts of the court decision. The analysis focuses on the obligations of service providers, forms of violations, losses suffered by users, and administrative, civil, and criminal liability. Conclusions are drawn deductively to establish the limits of service providers' legal responsibility and identify ways to strengthen personal data protection for users.

RESULTS AND DISCUSSION

Regulation of Personal Data Protection in the Implementation of Online Lending Services in Indonesia

Online lending services, legally recognized under Indonesian laws and regulations as LPBBTI, refer to the provision of financial services that facilitate direct funding transactions between lenders and borrowers through electronic systems (Financial Services Authority Regulation No. 40 of 2024). Unlike conventional bank lending, which generally relies on collateral and face-to-face interactions, online lending providers assess the creditworthiness of prospective borrowers almost entirely through personal data collected via digital applications, such as national identification numbers, facial photographs, bank account details, and transaction histories. Consequently, online lending providers, acting as Personal Data Controllers, bear legal obligations to protect such data (Theresa & Marlyna, 2024).

The legal framework governing personal data protection in online lending services is rooted in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees every person’s right to the protection of themselves, their family, honor, dignity, and property under their control. Since personal data is inherently connected to an individual’s identity, its protection constitutes a constitutional right that the state is obligated

to guarantee (Wijaya et al., 2023). At the data collection stage, the primary issue concerns the validity of consent. Article 20 of the PDP Law requires valid and explicit consent, while personal financial data and biometric data collected by online lending providers are classified as specific personal data under Article 4 of the PDP Law.

Consequently, much of the data processed in online lending activities requires a higher level of protection. In practice, consent within online lending applications is generally obtained through a single checkbox agreeing to lengthy terms and conditions. As a result, prospective borrowers who urgently need access to funds and seek a quick and convenient process often have little practical choice but to accept such terms (Kim et al., 2025). Furthermore, personal data processing must comply with the principles stipulated in Article 16 paragraph (2) of the PDP Law, including the requirements that data collection be limited, transparent, and lawful; processing be consistent with its intended purposes; data subjects' rights be guaranteed; data accuracy and accountability be maintained; data security be protected against unauthorized access or destruction; and data subjects be informed of the purposes of processing activities and the potential occurrence of personal data protection failures. For online lending providers, the purpose limitation principle means that data collected for creditworthiness assessments must not be used for other purposes, such as pressuring borrowers by contacting individuals listed in their mobile phone contacts (Kim et al., 2025).

Users, as data subjects, are also entitled to the rights stipulated in Articles 5 to 15 of the PDP Law, including the right to information, the right to access, rectify, and erase personal data, the right to withdraw consent, and the right to seek legal remedies and compensation. One provision particularly relevant to online lending concerns the prohibition of obtaining ambiguous consent, for example, by incorporating consent to personal data processing into general service terms and conditions, as well as prohibiting consent obtained through deceptive or misleading means (Kim et al., 2025). In addition, Article 26 paragraph (1) of the ITE Law stipulates that the use of any information through electronic media concerning an individual's personal data must be carried out with the consent of the person concerned. Article 26 paragraph (2) of the ITE Law further grants individuals who suffer losses the right to file a lawsuit.

More specifically, sectoral regulations governing the financial services industry are established under Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector ("**P2SK Law**"), which places LPBBTI activities under the regulation and supervision of OJK and emphasizes the obligation of financial service providers to maintain the confidentiality and security of consumer data. To implement these provisions, OJK issued Regulation Number 10/POJK.05/2022, which requires service providers to maintain the confidentiality, integrity, and availability of users' personal data and obtain the data owner's consent before using such data. These obligations had previously also been regulated under OJK Regulation Number 77/POJK.01/2016. However, a new issue arises because online lending transaction data is no longer stored exclusively by service providers but is also shared with OJK and industry associations through a two-way reporting system under OJK Regulation Number 8 of 2026. Although this data-sharing mechanism serves the purpose of preventing multiple overlapping loans, it also expands the number of parties possessing borrowers' personal data, thereby increasing the potential for misuse. Accordingly, the prohibition imposed on service providers and associations against disclosing or trading users' information under this regulation becomes particularly important (Otoritas Jasa Keuangan [OJK], 2026).

In the event of a personal data breach, Data Controllers are obligated to maintain data confidentiality, supervise processors acting on their behalf, and provide written notification no later than 3 x 24 hours following the occurrence of a personal data protection failure, as stipulated in Article 46 of the PDP Law. Violations of the obligations may result in administrative sanctions under Article 57 of the PDP Law, including administrative fines of up

to 2% of annual revenue. The PDP Law is further elaborated through its implementing regulation, Government Regulation Number 33 of 2026 concerning the implementing Regulations of Law Number 27 of 2022 on Personal Data Protection ("**Government Regulation 33/2026**").

The debt collection stage represents the point at which personal data violations most frequently occur. Several studies indicate that the disclosure of borrowers' personal data to family members and colleagues, sometimes accompanied by threats, constitutes a recurring pattern in online lending collection practices (Kurniawati & Yunanto, 2022). From a normative perspective, such practices violate the purpose limitation principle under Article 16 paragraph (2) of the PDP Law, as data initially provided for creditworthiness assessments is subsequently used to exert pressure on borrowers. Such practices also violate OJK Regulation Number 22 of 2023, which prohibits debt collection activities directed at parties other than consumers, as well as conduct involving threats or actions intended to humiliate consumers. Service providers cannot evade liability by arguing that debt collection activities were carried out by third parties. Under the PDP Law, debt collection agencies function as Personal Data Processors acting under the instructions of Data Controllers. Consequently, service providers remain responsible for the manner in which processors utilize personal data. Normatively, the regulatory framework for personal data protection in online lending services encompasses every stage of data processing. Nevertheless, borrowers whose personal data has been misused still lack legal certainty regarding the appropriate authority or institution to which they should submit their complaints.

Forms of Users' Personal Data Misuse in Online Lending Services

The development of online lending services has provided the public with easier access to financing without requiring lengthy procedures, as commonly found in conventional lending services. However, such convenience also raises legal concerns, particularly regarding the collection, use, and storage of users' personal data. In online lending services, users are generally required to provide information such as personal identification, telephone numbers, addresses, bank account information, and other data necessary for verification and creditworthiness assessments (Fikriana & Suhendra, 2023). Problems arise when such data is excessively collected, accessed without a lawful basis, or used for purposes inconsistent with the original purpose of its collection (Fritiana et al., 2025).

From a legal perspective, granting an application access to personal data cannot automatically be interpreted as unlimited consent for service providers to use all information available on users' devices. The PDP Law stipulates that personal data processing must have a lawful basis and comply with data protection principles. Article 20 of the PDP Law establishes the legal bases for personal data processing, while Article 16 paragraph (2) sets out the principles governing data processing, including purpose limitation, accuracy, security, and accountability in personal data processing (Fritiana et al., 2025). Therefore, the collection of information irrelevant to lending requirements or the use of data beyond its specified purposes may give rise to legal issues if it lacks a lawful basis for processing.

Personal data misuse during the collection and processing stages reflects the imbalance in the positions of users and online lending service providers. Users often lack adequate information regarding the types of data collected, the parties receiving such data, and the duration of its storage. Therefore, legal protection cannot rely solely on user consent but must also ensure transparency, purpose limitation, processing security, and service provider accountability. The legality of an online lending service does not automatically legitimize all data collection and usage practices carried out by the provider.

Personal data misuse in online lending services may occur through the extraction of users' contact lists (contact injection), which are subsequently used for debt collection

purposes. Such data may be exploited to send repeated messages via SMS or WhatsApp, make harassing phone calls, and convey misleading information to debtors' family members, friends, or colleagues. These practices demonstrate that personal information is no longer used solely for loan administration and verification purposes but has instead become a means of social pressure to compel debt repayment.

This issue becomes even more serious when third parties' personal data is used without a lawful basis, despite the fact that such parties have no legal relationship with the loan agreement. As a result, third parties may experience privacy violations, psychological distress, and even damage to their social relationships due to improper debt collection practices. Therefore, online lending service providers must ensure that the collection and use of personal data are carried out for lawful purposes and are not misused during debt collection processes. The engagement of debt collection agencies (debt collectors) does not absolve service providers of their responsibility to supervise personal data processing activities conducted for the purposes of their business operations.

Another form of personal data misuse may occur through data breaches resulting from inadequate security systems, unauthorized access, or actions by internal parties who abuse their authority. In their research, Evi Nurani, Wiryanto, and Slamet Riyanto found that data breaches in online lending services may be associated with inadequate data security management, hacking of data storage centers, as well as misuse by company employees and illegal cooperation with debt collectors (Nurani et al., 2023). These findings indicate that the risk of data misuse does not arise solely during data collection, but also during the storage and management of data by service providers.

Data breaches may lead to further consequences, including the dissemination of personal information, fraud, and the use of individuals' identities without their knowledge or consent. Research conducted by Glory Sylviana and other authors also examines the risk of data breaches involving e-wallet users, whereby such data may potentially be misused for online lending purposes (Sylviana et al., 2024). This situation demonstrates that data security constitutes an essential component of consumer protection in digital financial services. Service providers must ensure that data storage systems, internal access restrictions, and supervision of parties handling personal data are adequately implemented.

In addition to data breaches, personal data misuse may also occur when users' contact lists are exploited for debt collection purposes by contacting individuals who have no legal relationship with the loan agreement. Erni Nur Shofiyah and Indri Fogar Susilowati describe practices of personal data misuse in peer-to-peer lending services, including contacting individuals listed in borrowers' contact lists beyond those designated as emergency contacts and informing them that the users have outstanding debts (Shofiyah & Susilowati, 2019). Such practices demonstrate that contact data stored on users' devices may be exploited to extend debt collection pressure to other parties.

The use of contact data for such purposes raises legal concerns because individuals whose phone numbers are stored on a debtor's device do not automatically consent to the processing of their personal data by online lending service providers. Third parties also do not automatically have an obligation to repay a debt merely because they are contacted by debt collectors. In certain circumstances, disclosing information about a debt to family members, friends, or colleagues may infringe upon privacy and damage the reputation of both the debtor and the individuals contacted. Therefore, the use of contact lists must be distinguished from the use of emergency contacts, which serves a limited purpose, and must be assessed based on the lawful basis for personal data processing and the debt collection methods employed.

The processing of personal data in online lending services also requires particular attention when it involves third parties, such as business partners, technology providers, or debt collection agencies. There is a risk of personal data misuse arising from illegal cooperation

between online lending service providers and debt collection groups. These findings highlight the importance of supervising parties granted access to users' personal data, particularly when such data is used for debt collection activities.

Legal issues arise when personal data initially provided for identity verification and creditworthiness assessment is subsequently used for other purposes that are inconsistent with the original basis for processing. The use of such data for operational purposes cannot be justified merely because the recipient has a business relationship with the service provider. It is necessary to assess whether such processing has a lawful basis, is consistent with the specified purposes, and continues to protect the rights of data subjects. In this context, Article 16 paragraph (2) and Article 20 of the PDP Law may serve as a basis for analyzing the principles governing personal data processing and the lawful basis for the use of such data.

The Legal Liability of Online Lending Service Providers for the Misuse of Users' Personal Data

The legal liability of online lending service providers for the misuse of users' personal data cannot be assessed solely based on whether the providers directly engage in such misuse, but must also consider their position and obligations as parties determining the purposes and means of personal data processing. In the provision of LPBBTI, service providers collect and process various types of users' personal data for identification, verification, funding eligibility assessments, transaction monitoring, and debt collection. Therefore, their control over such data gives rise to a legal obligation to ensure that its processing is lawful, limited to specified purposes, and supported by adequate security systems. This position is further reinforced by the enactment of the PDP Law, which stipulates that Personal Data Controllers are responsible for personal data processing and must demonstrate accountability in fulfilling personal data protection principles, as provided under Article 47.

These obligations do not cease once personal data has been collected from users. Article 37 of the Personal Data Protection Law requires Personal Data Controllers to supervise every party involved in processing personal data under their control, while Article 39 requires Personal Data Controllers to prevent unauthorized access to personal data. Accordingly, the liability of service providers has a preventive dimension, namely the obligation to establish control mechanisms capable of preventing misuse before any harm occurs (Basmah & Priyanto, 2023).

In the context of online lending, these obligations may be implemented through restrictions on access rights to users' personal data, authentication of parties accessing the system, recording of data processing activities, supervision of employees and third parties, and revocation of access rights upon the termination of employment relationships. This framework is relevant to the issues examined in this study, as personal data misuse does not necessarily originate from external parties but may also be committed by individuals who previously obtained legitimate access through their employment relationships (Rizkillah et al., 2024).

These preventive obligations are further reinforced by sector-specific regulations under POJK 40/2024. This regulation stipulates that service providers must obtain the consent of Personal Data owners to collect and use their personal data, subject to exceptions provided under applicable laws and regulations. Furthermore, users have the right to access and obtain copies of their personal data, request corrections to inaccurate data, and request the destruction of personal data submitted to service providers. POJK 40/2024 also establishes obligations for service providers to ensure proper data management throughout the entire data lifecycle, from collection to destruction. Accordingly, the legal relationship between users and service providers does not merely constitute a relationship between funders and funding recipients, but also encompasses a legal relationship concerning the processing and protection of personal data.

In the event of a personal data protection failure, service providers may also incur liability based on their notification and recovery obligations. Article 46 of the PDP Law requires Personal Data Controllers to provide written notification to the Personal Data Subject and the competent authority no later than 3 × 24 hours after becoming aware of the personal data protection failure. Such notification must at least include the personal data that has been disclosed, the time and manner in which the data was disclosed, and the measures taken to address and recover from the incident. This provision demonstrates that the liability of service providers does not arise solely when they are proven to have actively disclosed personal data, but also encompasses the obligation to respond appropriately to security failures resulting in users' data being exposed or accessed without authorization.

Furthermore, the liability of service providers may be examined from an administrative perspective. Article 57 of the Personal Data Protection Law stipulates that violations of certain obligations imposed on Personal Data Controllers may be subject to administrative sanctions, including written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines. Such fines may reach a maximum of 2% of annual income or revenue in relation to the relevant violation variable. In the context of LPBBTI, these obligations operate alongside the OJK regulatory authority to supervise service providers. Therefore, violations of data security and governance obligations may result in administrative consequences under both the personal data protection framework and OJK sector-specific regulations. This is consistent with the research conducted by Yuga and Hummerson, which demonstrates that online lending service providers, as electronic system operators, are obligated to ensure reliable and secure systems, establish a lawful basis for data processing, provide information to data subjects, and maintain the confidentiality and security of consumer data (Yuga & Hummerson, 1972).

From a civil law perspective, the misuse of personal data resulting in losses may also provide grounds for users to claim compensation. The PDP Law explicitly grants Personal Data Subjects the right to file claims and receive compensation for violations involving the processing of their personal data. Accordingly, if a breach of data protection obligations, the losses suffered by users, and the causal relationship between the breach and such losses can be established, service providers may be held civilly liable. In the context of personal data misuse, losses may include both economic and non-economic damages, such as violations of privacy, damage to reputation, threats to security, and disruption of users' comfort resulting from the disclosure of data to unauthorized parties. Victims of personal data theft involving online lending services are afforded legal protection under the PDP Law, the ITE Law, and Law Number 8 of 1999 concerning Consumer Protection. Nevertheless, the mechanisms for obtaining compensation remain an issue that requires further clarification (Kiasatina et al., 2025).

Meanwhile, criminal liability must be distinguished between the liability of individual perpetrators and that of corporations. The PDP Law stipulates that any person who intentionally and unlawfully obtains, discloses, or uses personal data that does not belong to them may be subject to criminal penalties under Article 67. Furthermore, where certain criminal offenses are committed by a corporation, Article 70 of the PDP Law allows criminal liability to be imposed on corporate management, controlling parties, individuals issuing orders, beneficial owners, and/or the corporation itself. Corporate criminal liability may result in fines of up to ten times the maximum fine prescribed for the relevant offense. This demonstrates that the law does not exclusively place responsibility on individuals who directly misuse personal data as the sole parties subject to criminal liability. Nevertheless, the application of criminal liability to service providers as corporations must take into account the legal construction of the offense, the parties exercising control, the form of culpability, and the relationship between the conduct and the corporation's business activities.

This issue can be examined through Central Jakarta District Court Decision Number 597/Pid.Sus/2021/PN.Jkt.Pst, which serves as the case study in this research. In this case, Michael Lisardo and Sunandar, who had previously been involved in debt collection activities at a fintech company, used customer contact data that remained in their possession after their employment relationships had ended. The data was used to carry out fictitious debt collection activities and threaten victims with the disclosure of their personal information. The court subsequently found both defendants guilty of committing criminal offenses under Article 28 paragraph (1) in conjunction with Article 45 paragraph (2) of the ITE Law, as applied in the decision, and imposed criminal penalties on each defendant. Meanwhile, PT Malkom Burung Indonesia and PT Zeus Indonesia were not among the parties sentenced by the court.

The decision highlights a broader issue concerning the boundaries of liability between individuals who misuse personal data and companies that control and process such data. In this case, the focus of liability was placed on the individual conduct of using personal data for fictitious debt collection activities and making threats against customers. However, as discussed in this research, the decision did not specifically examine whether the companies had fulfilled their preventive obligations to revoke former employees' access rights, control copies of personal data, and supervise data usage after the termination of employment relationships. Nevertheless, under Articles 37 and 39 of the PDP Law, Personal Data Controllers are required to supervise parties involved in data processing and prevent unauthorized access. Therefore, the termination of an employee's employment relationship does not automatically extinguish the service provider's obligation to ensure that data previously under its control can no longer be accessed or used unlawfully.

Accordingly, the liability of online lending service providers should be established based on the principle of accountability, which positions service providers not merely as parties responsible when they directly engage in data misuse, but also as parties obligated to demonstrate that all personal data processing activities have been carried out lawfully and securely. A study on corporate liability for the dissemination of personal data belonging to online lending customers, published in 2025, also identifies the PDP Law as an important legal basis for assessing corporate liability for the disclosure of customers' personal data (Oktaviani et al., 2021). In this context, service providers must be able to demonstrate the implementation of adequate data governance, including access controls, supervision of employees and third parties, and incident response procedures. This approach also prevents two extremes in determining legal liability. First, placing all responsibility on individuals who misuse personal data without examining potential failures in the company's internal control systems. Second, automatically imposing liability on service providers for every instance of individual misconduct without considering the elements of fault and the causal relationship between the misconduct and the resulting harm.

Based on the foregoing discussion, the legal liability of online lending service providers for the misuse of users' personal data can be constructed through three liability regimes: administrative, civil, and criminal. Administrative liability serves to ensure service providers' compliance with data governance and security obligations; civil liability provides a mechanism for compensating users who have suffered losses; while criminal liability addresses acts of data misuse that fulfill the elements of a criminal offense, including the possibility of corporate criminal liability under the PDP Law. Practices involving threats, data disclosure, and doxing by debt collection parties may also constitute separate criminal offenses (Fajira & Nurfatlah, 2026). Therefore, effective legal protection cannot rely solely on the imposition of sanctions after misuse has occurred. Instead, service providers' preventive obligations must be positioned as a fundamental component of the legal liability framework.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Personal data protection in online lending services in Indonesia is regulated under the PDP Law and POJK 40/2024. Both regulations emphasize the responsibility of service providers, as Personal Data Controllers, to ensure that personal data is processed lawfully, for specific purposes, and securely. These responsibilities include supervising all parties involved in data processing and preventing unauthorized access. Therefore, user consent does not justify the use of personal data beyond its original and lawful purpose. The misuse of personal data in online lending services can occur through excessive data collection, the use of data beyond its original purpose, unauthorized access, data leaks, and the distribution of private information to pressure borrowers during debt collection. Such practices can cause financial losses, privacy violations, reputational damage, and psychological distress to both users and third parties. An analysis of Central Jakarta District Court Decision Number 597/Pid.Sus/2021/PN.Jkt.Pst. shows that customer data still held by a former employee can be misused for fraudulent debt collection and threats to distribute private information. This case highlights the importance of proper data control, including after an employment relationship has ended.

The legal responsibility of online lending providers can be examined from administrative, civil, and criminal perspectives. Administrative responsibility relates to violations of data governance and security obligations, while civil liability provides users with a legal basis to claim compensation when the relevant legal requirements are met. Criminal liability for individuals or corporations depends on whether the elements of a criminal offense are fulfilled under the applicable laws. Therefore, service providers cannot automatically avoid responsibility simply because the misuse was carried out by employees or third parties. However, their liability must also be based on their legal obligations, proven fault, and a relevant causal connection, rather than solely on the occurrence of data misuse. This study shows that effective personal data protection does not depend only on taking action against offenders after a violation has occurred. It also requires service providers to take preventive measures. These measures include restricting access rights, recording data processing activities, supervising employees and third parties, and revoking access while controlling remaining copies of data after employment relationships end. In addition, complaint procedures and mechanisms for restoring users' rights need to be made clearer to ensure effective legal protection. A balanced approach to legal responsibility must ensure accountability from service providers, protect users' rights, and maintain legal certainty through a proper assessment of the applicable legal responsibilities.

Limitations

This study has several limitations. First, it employs a normative legal research method based primarily on statutory regulations, legal literature, and a single court decision, namely Central Jakarta District Court Decision No. 597/Pid.Sus/2021/PN.Jkt.Pst. Therefore, the findings may not fully represent the various forms of personal data misuse and legal liability that occur in the broader online lending industry. Second, the analysis focuses on the Indonesian legal framework, particularly PDP Law and POJK 40/2024, without conducting empirical investigations into the actual implementation of these regulations by online lending providers. Third, the study primarily examines administrative, civil, and criminal liability, while other practical aspects, such as institutional coordination, enforcement mechanisms, and the effectiveness of remedies available to affected users, require further examination.

Recommendations

Future research should expand the analysis by examining a broader range of court decisions involving personal data misuse in online lending services to provide a more comprehensive

understanding of the legal liability of providers and other parties involved in data processing. Further studies may also incorporate empirical research, including interviews with affected users, online lending providers, regulators, and law enforcement authorities, to evaluate the implementation and effectiveness of existing personal data protection regulations. In addition, future research should further explore the mechanisms for enforcing administrative, civil, and criminal liability, particularly regarding corporate accountability for misconduct committed by employees or third-party service providers. Greater attention should also be given to strengthening preventive measures, including access control, internal monitoring, data security governance, and the revocation of data access following the termination of employment relationships.

Author Contributions

All authors made significant contributions to this study. Sascha Kezia Cenniago, Vanessa Maurent, Beatrice Callista Yo, Stephanie Sigrid, Owen Edgar Kuncoro, and Pietro Grassio Ekoyulio collectively contributed to the conceptualization of the research, development of the theoretical framework, identification and collection of legal materials, legal analysis, interpretation of findings, and preparation of the manuscript. All authors participated in reviewing and revising the manuscript and approved the final version for publication. All authors agree to be accountable for the accuracy and integrity of the work.

REFERENCES

Basmah, H., & Priyanto, I. M. D. (2023). Perlindungan hukum terhadap data pribadi dalam layanan pinjaman online. *Jurnal Kertha Desa*, *11*(4). https://ojs.unud.ac.id/index.php/kerthadesa/article/view/97505/49319

Bisnis.com. (2026, August 29). Aturan turunan UU PDP: Persetujuan data konsumen lebih ketat. https://teknologi.bisnis.com/read/20260829/84/1999753/aturan-turunan-uu-pdp-persetujuan-data-konsumen-lebih-ketat

Fajira, E., & Nurfatlah, T. (2026). Pertanggungjawaban pidana tindakan pengancaman dan penyebaran data pribadi yang dilakukan oleh debt collector pinjaman online. *Jurnal Parhesia*, *4*(1). https://doi.org/10.29303/zg7n6k25

Fikriana, A., & Suhendra. (2023). Praktik finansial teknologi ilegal dalam bentuk pinjaman online ditinjau dari etika bisnis. *JUSTICES: Journal of Law*, *2*(4), 231–232. https://doi.org/10.58355/justices.v2i4.94

Fritiana, A., Daishahwa, & Wiraguna, S. A. (2025). Penyalahgunaan data pribadi pada layanan pinjaman online: Analisis perlindungan dan sanksi hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(2), 523–529. https://doi.org/10.61104/alz.v3i2.1082

Hanifawati, S. D. (2021). Urgensi penegakan hukum pidana pada penerima pinjaman kegiatan peer to peer lending fintech ilegal dan perlindungan data pribadi. *Jurnal Penegakan Hukum dan Keadilan*, *2*(2), 162–172. https://doi.org/10.18196/jphk.v2i2.12181

Kiasatina, O. S., Wulandari, L., & Amin, I. (2025). Perlindungan hukum terhadap pengguna pinjaman online yang menjadi korban tindak pidana pencurian data pribadi. *Jurnal Parhesia*, *3*(1). https://journal.unram.ac.id/index.php/Parhesia/id/article/view/6464/3518

Kim, M. T., Jacob, Y. M. Y., & Bire, C. M. D. (2025). Perlindungan data pribadi pada platform digital pinjaman online ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Studi kasus di Kota Kupang, NTT). *Artemis Law Journal*, *2*(2), 511–526. https://doi.org/10.35508/alj.v2i2.21070

Kurniawati, H., & Yunanto. (2022). Perlindungan hukum terhadap penyalahgunaan data pribadi debitur dalam aktivitas pinjaman online. *Jurnal Ius Constituendum*, *7*(1), 102–114. https://doi.org/10.26623/jic.v7i1.4290

Nurani, E., Wiryanto, & Riyanto, S. (2023). Optimalisasi perlindungan konsumen atas kebocoran pengelolaan data pribadi dalam pinjaman online. *Jurnal Hukum Jurisdictie, 5*(2), 51–69. https://doi.org/10.34005/jhj.v5i2.133

Oktaviani, A. N., Fauziah, & Salamah, A. (2021). Pertanggungjawaban korporasi terhadap penyebaran data pribadi nasabah pinjaman online menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Jurnal Hukum Jurisdictie, 7*(2). https://doi.org/10.34005/jhj.v7i2.187

Otoritas Jasa Keuangan. (2026a). *OJK terbitkan POJK Nomor 8 Tahun 2026, atur pelaporan dan permintaan data transaksi industri Pindar* [Siaran pers SP 149/2026].

Otoritas Jasa Keuangan. (2026b). *Siaran pers: Stabilitas sektor jasa keuangan terjaga di tengah meningkatnya tekanan terhadap kinerja perekonomian global* [Siaran pers SP 109/DKPU/OJK/VI/2026]. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/RDKB-Mei-2026.aspx

Priliasari, E. (2019). Pentingnya perlindungan data pribadi dalam transaksi pinjaman online. *Majalah Hukum Nasional, 49*(2), 1–27. https://doi.org/10.33331/mhn.v49i2.44

Rizkillah, R., Basri, Kurniaty, Y., & Hakim, H. A. (2024). Pertanggungjawaban tindak pidana doxing oleh debt collector pinjaman online dalam penagihan hutang nasabah. *Borobudur Law and Society Journal, 3*(2). https://doi.org/10.31603/11708

Shofiyah, E. N., & Susilowati, I. F. (2019). Penyalahgunaan data pribadi penerima pinjaman dalam peer to peer lending. *Novum: Jurnal Hukum, 6*(2). https://doi.org/10.2674/novum.v6i2.30092

Sylviana, G., Setiawan, D. A., Listyani, C., Apriyanti, E. K., & Putri, L. A. P. (2024). Perlindungan hukum data pengguna e-wallet atas kebocoran data yang disalahgunakan oleh pinjaman online. *Journal Evidence of Law, 3*(3), 340–353. https://doi.org/10.59066/jel.v3i3.765

Theresa, G., & Marlyna, H. (2024). Pelindungan data pribadi pada layanan pendanaan berbasis teknologi informasi pasca Undang-Undang Nomor 27 Tahun 2022 dan Undang-Undang Nomor 4 Tahun 2023. *Jurnal Hukum & Pembangunan, 54*(2), 227–258. https://doi.org/10.21143/jhp.vol54.no2.1631

Wijaya, M. R., Emilson, N. H., & Nawawi, K. (2023). Perlindungan subjek hukum dalam perkembangan teknologi ditinjau dari perspektif hukum dan hak asasi manusia. *Marwah Hukum, 1*(1), 21–28. https://doi.org/10.32502/mh.v1i1.5599

Yuga, R. I., & Hummerson, A. W. (1972). Tanggung jawab penggunaan data pribadi oleh penyelenggara sistem elektronik dalam layanan pinjaman online. *Amicus Curiae, 2*(1). https://doi.org/10.25105/ncewzp73