Requisitoire : Law Enforcement
Vol. 18, No. 1, July 2026, pp. 53~60
ISSN: 2986-3988 (Online), DOI: 10.59651/relae

Legal protection of personal data in information technology-based online loans via the UangMe Application

Widarta Adiadhma[1], Sufiarina[2], Wira Utama[3]
[1,2,3]Faculty of Law, Universitas Tama Jagakarsa, Jakarta, Indonesia

Article Info

Article history:

Received : Jul 19, 2026
Revised : Aug 17, 2026
Accepted : Sept 02, 2026

Keywords:

Lending and Borrowing;
Online Loans;
Privacy;
Personal Data Protection;
UangMe.

ABSTRACT

The expansion of information technology-based lending has increased access to credit while intensifying the processing of borrowers' personal data. This study examines legal protection for borrowers' personal data and the legal responsibility of an online lending provider through the UangMe application. The research uses normative juridical legal research with statutory and case approaches. Primary legal materials include Law Number 27 of 2022 on Personal Data Protection, Law Number 8 of 1999 on Consumer Protection, Law Number 1 of 2024 on Electronic Information and Transactions, Financial Services Authority Regulation Number 22 of 2023, and the currently applicable Financial Services Authority Regulation Number 40 of 2024 on Information Technology-Based Joint Funding Services. Case materials consist of documented public user complaints concerning data deletion, transparency, access to device data, debt-collection pressure, and complaint handling. The findings show that Indonesia already provides a multi-layered protection framework, but effective protection depends on data minimization, transparent processing, accurate records, effective deletion mechanisms, secure complaint channels, and enforceable supervision. The UangMe-related complaints used in this research are treated as allegations and indicators of legal risk rather than adjudicated violations. Where a violation is proven, provider responsibility may arise through administrative sanctions, civil compensation, and other consequences available under personal data and consumer protection law. The study contributes a case-based mapping between user complaint patterns and the current post-2024 regulatory framework.

Corresponding Author:

Widarta Adiadhma
Faculty of Law, Universitas Tama Jagakarsa
Jl. Letjen T.B. Simatupang No. 152, Tanjung Barat, Jagakarsa, Jakarta Selatan 12530, Indonesia
Email: adiadhma88@gmail.com.

1. INTRODUCTION

Digital lending has become a prominent component of Indonesia's financial technology ecosystem because it connects funders and borrowers through electronic systems and can reduce geographic and procedural barriers to credit. This convenience, however, is inseparable from intensive personal-data processing. Identity information, contact details, financial information, device-related data, and biometric verification may be collected at different stages of registration, credit scoring,

disbursement, and collection. Personal data therefore performs a dual role: it supports risk assessment and fraud prevention, but it also creates legal exposure when processing is excessive, opaque, inaccurate, insecure, or disconnected from the original purpose for which the data was obtained.

Recent legal scholarship consistently places personal-data governance at the center of fintech-lending consumer protection. Angeline & Dwijayanthi, (2023) emphasize lawful consent and the duties of fintech providers as data controllers. Syahruddin & Zulfa, (2024) identify institutional and enforcement issues surrounding personal-data violations in fintech lending. Rohendi & Kharisma, (2024) argue that regulatory protection must be complemented by effective institutional arrangements and consumer literacy. Rahmawati et al., (2024) map misuse risks such as unauthorized use and unlawful disclosure, while Novelin et al., (2025) underline stronger supervision and public awareness. In a related context, Priambono et al., (2024) demonstrate that debt-collection practices can generate personal-data leakage risks. These studies establish a strong general framework, but most address fintech lending at sector level rather than linking specific complaint patterns from one licensed platform to the updated regulatory structure.

The UangMe application provides a relevant case for that purpose. The undergraduate research from which this article is developed records UangMe as a service operated by PT Uangme Fintek Indonesia under OJK licensing and documents public user complaints posted in 2025. The source material describes registration and verification processes involving identification data, telephone number, email address, identity-card images, selfies, employment and income information, geolocation, and other device permissions. It also records complaints concerning the difficulty of deleting data after a rejected or completed loan, changing application policies, unclear account obligations, pressure during collection, and inadequate responses from customer service. Because these materials are user-generated complaints, they cannot by themselves prove a statutory violation; they are used here as factual indicators for normative legal analysis.

The regulatory context has also changed since the thesis was prepared. Law Number 27 of 2022 on Personal Data Protection establishes rights of data subjects and obligations of personal-data controllers and processors. Financial Services Authority Regulation Number 22 of 2023 strengthens consumer protection in the financial services sector, including confidentiality and security of consumer data and responsible collection practices. Most importantly, Financial Services Authority Regulation Number 40 of 2024 on Information Technology-Based Joint Funding Services (LPBBTI) has been effective since 27 December 2024 and revoked Financial Services Authority Regulation Number 10 of 2022, although implementing provisions remain applicable insofar as they do not conflict with the new regulation. Accordingly, an article intended for current publication should not reproduce the thesis's regulatory analysis without harmonizing it with the post-2024 framework.

The gap addressed in this article is therefore the absence of a focused mapping between UangMe-specific user complaint indicators and the current architecture of personal-data, consumer-protection, civil-liability, and LPBBTI regulation. This mapping is important because a provider's formal licensing status does not eliminate the need for continuous compliance in each stage of data processing. Conversely, public complaints should not be converted into findings of wrongdoing without legal proof. A balanced legal analysis must distinguish licensing, compliance duties, evidentiary status, and potential liability.

This study consequently addresses two questions: how does Indonesian law protect the personal data of online-lending borrowers in the context of the UangMe application, and what forms of legal responsibility may arise for the provider if misuse is proven? The article's novelty lies in combining complaint-based case indicators from the 2025 UangMe materials with the current regulatory framework, especially the transition to Financial Services Authority Regulation Number 40 of 2024. The objective is not to adjudicate the complaints, but to formulate a legally accurate protection and accountability map that can guide providers, consumers, regulators, and further research.

2. METHOD

This research applies normative juridical legal research. It examines legal norms, principles, and regulatory relationships relevant to the processing of personal data in online lending through statutory and case approaches. The primary legal materials consist of binding legal sources: the Civil Code,

Law Number 8 of 1999 on Consumer Protection(UU RI, 1999), Law Number 27 of 2022 on Personal Data Protection(UU RI, 2022), Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law(UU RI, 2024), Financial Services Authority Regulation Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector(OJK, 2023), and Financial Services Authority Regulation Number 40 of 2024 on LPBBTI(OJK, 2024). Financial Services Authority Regulation Number 10 of 2022 is used only as a historical regulatory reference because it has been revoked by the 2024 regulation. Secondary legal materials consist of peer-reviewed journal articles, scholarly books, doctoral research, and other academic literature relevant to personal-data protection, fintech lending, consumer protection, and legal responsibility. No tertiary legal materials, such as legal dictionaries or encyclopedias, are used in the analysis.

Legal materials were collected through document and literature study. Statutes and OJK regulations were traced through official legal and regulatory sources, while secondary materials were identified from scholarly publications and the bibliography of the underlying research. As supplementary factual sources, this study uses three public reviews of the UangMe application documented in the underlying thesis and attributed to Ari Parikesit, Wina Widianingsih, and Dede Sopan Apiatna (Apiatna, 2025; Parikesit, 2025; Widianingsih, 2025). The reviews were purposively selected as case materials because they directly raised legally relevant issues concerning transparency and complaint handling, retention or deletion of personal data, and account-data accuracy. The study does not treat all Google Play Store reviews as a population and does not claim that the three reviews statistically represent all users. Only these three complaints were used because the research is normative juridical and employs complaint documents as focused indicators for legal-issue mapping rather than as a quantitative sample.

The complaint documentation covers public reviews posted in 2025, including reviews dated 3 May 2025 and 21 June 2025, and the materials were accessed and documented in July 2025. For methodological credibility, the reviews are used only when they are traceable to the public application-review context, contain an identifiable reviewer name and date where available, and are consistently recorded in the underlying thesis; their credibility is limited to documenting the existence and content of a complaint, not proving the truth of the alleged conduct. The materials are complemented by scholarly literature and official OJK regulatory information. Legal materials are analyzed qualitatively through statutory interpretation, systematic interpretation, and legal argumentation. The analysis proceeds in four stages: identifying the data-processing activity or complaint pattern; classifying the relevant right or duty; linking the issue to the applicable regulatory layer; and determining the potential legal consequence if the elements of a violation, loss, causation, and responsibility are established. This sequence preserves the normative character of the research while preventing allegations from being presented as established facts.

3. RESULTS AND DISCUSSION

3.1 UangMe Data Processing and Regulatory Position

The UangMe materials illustrate why personal-data protection in digital lending must be understood as a life-cycle obligation rather than a single consent event. Data are obtained during account creation and identity verification, used for credit assessment and fraud controls, retained during the contractual relationship, and may remain relevant for legally permitted retention periods after the transaction ends. Each stage requires a valid legal basis, a defined purpose, proportional processing, adequate security, data accuracy, and a mechanism for exercising data-subject rights. Where biometric or financial data are involved, the potential impact of misuse is particularly serious because such data can facilitate identity fraud, profiling, reputational harm, or financial loss.

More specifically, the right to terminate processing and to erase or destroy personal data is recognised under Article 8 of Law No. 27 of 2022 on Personal Data Protection (PDP Law) and is further implemented through Articles 42–45. This right is not absolute. Articles 15 and 50 provide limited exceptions, including for law enforcement, public administration, and financial-sector supervision, while Article 16(2)(g) permits continued retention where otherwise required by legislation. Article 20(2)(c) also recognises compliance with a legal obligation as a lawful basis for processing. Accordingly, an LPBBTI provider may refuse or defer a deletion request only to the extent that retention remains necessary to comply with a specific statutory obligation, financial supervision, an audit, or an ongoing legal process. These exceptions do not provide the provider with unrestricted

commercial discretion; the applicable legal basis and necessity for continued retention must be identifiable and documented.

Under Article 165(1) of OJK Regulation No. 40 of 2024, an LPBBTI provider must retain personal data in its electronic system for at least five years after the business relationship ends. This provision establishes a minimum retention period rather than a uniform maximum period. Retention beyond that period must therefore remain supported by another applicable legal obligation or a specific and lawful purpose. Once the relevant retention period and legal necessity have expired, the data must be erased or destroyed in accordance with Articles 43–45 of the PDP Law. Article 165(2)–(6) of OJK Regulation No. 40 of 2024 further requires the provider to establish a deletion mechanism and permits deletion where, among other circumstances, the data were unlawfully processed, are no longer consistent with the original purpose, have exceeded the permitted period of use, have caused harm, or relate to a business relationship that has ended and is no longer governed by the agreement.

Any refusal should be communicated in writing and should identify the legal basis, the categories of data retained, the remaining retention period, and the available complaint or review mechanism. The PDP Law and Article 165 of OJK Regulation No. 40 of 2024 do not expressly establish a standalone sanction solely for failing to provide reasons for a deletion refusal; this constitutes a point of regulatory ambiguity. Nevertheless, an unexplained refusal may be inconsistent with the transparency and accountability principles under Articles 16(2) and 47 of the PDP Law. Where the deletion request is submitted as a consumer complaint, the Elucidation of Article 76(1) of OJK Regulation No. 22 of 2023 requires a rejection to be communicated together with its reasons. A failure to provide an adequate complaint response may engage the administrative enforcement mechanism under Article 77, while an unlawful substantive failure to erase data may result in administrative sanctions under Article 57 of the PDP Law and a claim for compensation under Article 12.

The fact that an LPBBTI provider is licensed is legally significant because licensing subjects the provider to OJK supervision and sectoral obligations. It is not, however, a conclusive statement that every operational practice is compliant. Compliance is continuous and activity-specific. The appropriate legal question is therefore not whether UangMe is a licensed platform, but whether each contested processing activity, retention decision, disclosure, and collection practice satisfies the duties imposed by personal-data and financial-services law.

3.2 Complaint-Based Indicators of Personal Data Misuse

Three complaints documented in the thesis provide a focused illustration of recurring legal-risk patterns. Table 1 summarizes the complaint-based indicators and the legal questions they generate. The descriptions retain the status of allegations and do not attribute a proven violation to UangMe.

Table 1. Complaint-based indicators and corresponding legal issues

Source	Complaint indicator	Primary legal issue	Normative implication
Ari Parikesit (3 May 2025)	Policy or system changes allegedly occurred without adequate notice; difficulty obtaining a substantive customer-service solution.	Transparency, good faith, complaint handling, and consumer information rights.	The provider should document notices, contractual changes, complaint responses, and the basis for any operational action.
Wina Widianingsih (2025)	Loan application was reportedly rejected, but the user stated that previously submitted personal data could not be deleted.	Purpose limitation, retention, deletion rights, and accountability.	Retention requires a continuing lawful basis; a rights request should receive a clear, auditable decision and explanation.
Dede Sopan Apiatna (21 June 2025)	The user reported no outstanding debt but alleged that permanent account deletion was blocked because the system showed an undefined obligation.	Data accuracy, account status, erasure, and system accountability.	Transaction history and debt status should be accurate, reconcilable, and capable of supporting a reasoned decision on deletion.

Across the three user reviews, which are used in this study as indicators of possible factual and legal issues rather than as judicial cases, three concerns are directly identifiable. First, the reviews by Wina Widianingsih and Dede Sopan Apiatna indicate possible difficulties in exercising data-deletion or account-closure rights after a loan application has been rejected or a debt is considered settled. Second, Ari Parikesit's review indicates a possible transparency problem arising from changes to platform rules without adequate notice. Third, the reviews indicate that ineffective

customer-service responses may weaken users' practical ability to obtain information and exercise their rights. Two additional concerns the proportionality of device permissions and the use of personal information in debt-collection activities remain legally relevant in the fintech-lending context. However, because these practices are not directly established by the three reviews, they must be treated as contextual risks requiring independent evidence rather than as proven practices of UangMe.

These concerns are consistent with the broader literature. Angeline & Dwijayanthi, (2023) connect fintech data processing with the requirements of valid consent and controller responsibility; Syahruddin & Zulfa, (2024) emphasize the importance of enforcement, while Novelin et al., (2025) identify unauthorized use and disclosure as central fintech-lending risks. The UangMe case materials add a platform-specific perspective by showing that the practical problem is not limited to data leakage.

identify unauthorized use and disclosure as central risks in fintech lending. The UangMe user-review materials add a platform-specific perspective by indicating that potential data-protection problems are not limited to data leakage. Retention, accuracy, transparency, the scope of data access, debt-collection practices, and complaint resolution are also relevant components of legal protection. Nevertheless, the reviews do not, by themselves, constitute conclusive evidence that UangMe has violated personal-data-protection law.

The reported experiences must be assessed against the specific rights provided under Law No. 27 of 2022 on Personal Data Protection (PDP Law). Articles 5–13 provide data subjects with, among other things, the rights to obtain information concerning the processing of their data, correct or update inaccurate data, access and obtain copies of their data, terminate processing and request deletion or destruction, withdraw consent, object to decisions based solely on automated processing, restrict processing, claim compensation, and exercise data portability. Account closure and data deletion must be distinguished because the termination of access to an account does not necessarily require the immediate destruction of every record where a statutory retention obligation remains applicable.

To the extent that UangMe determines the purposes and means of processing personal data, it acts as a Personal Data Controller. It must therefore identify a lawful basis for every processing activity under Article 20 of the PDP Law. It must also ensure that processing is limited, specific, lawful, transparent, consistent with the stated purpose, accurate, secure, and accountable. These obligations include providing clear information to users, facilitating the exercise of data-subject rights, maintaining an appropriate retention schedule, correcting inaccurate records, responding to requests, and deleting or destroying data when the applicable retention period or processing purpose has ended. Consent does not constitute a blanket authorization for all subsequent processing, and it is only one of the lawful bases recognized by the PDP Law.

The right to deletion is not absolute. Articles 15 and 50 of the PDP Law provide limited exceptions for specified public-interest functions, although these provisions do not create a general exemption for digital-lending platforms. A deletion request may also be refused or postponed when the controller must retain particular records to comply with a legal obligation. For an LPBBTI provider, Article 165 of OJK Regulation No. 40 of 2024 requires relevant personal data and documents to be retained in the electronic system for at least five years after the business relationship ends. Article 63 of OJK Regulation No. 8 of 2023 also requires financial-service providers to retain certain customer-due-diligence records relating to prospective customers, customers, and walk-in customers for at least five years. Therefore, some identification and KYC records relating to a rejected applicant may remain subject to mandatory retention even when no loan is ultimately granted.

These sectoral obligations may provide UangMe with a lawful basis under Article 20(2)(c) of the PDP Law, namely processing that is necessary for compliance with a legal obligation. In Wina Widianingsih's situation, the rejection of a loan application does not automatically eliminate every legal basis for retaining required identification or due-diligence records. Similarly, in Dede Sopan Apiatna's situation, settlement of a loan may mark the beginning of the applicable retention period rather than create an immediate obligation to destroy all records. However, these provisions do not authorize UangMe to retain every category of data indefinitely or to use retained data for unrelated commercial, profiling, marketing, or collection purposes. UangMe would need to identify the specific records covered by the retention obligation, the legal purpose of the retention, the date on which the retention period commenced, and the date on which the data would become eligible for deletion.

The five-year requirement is a minimum statutory period and should not be interpreted as authorization for unlimited retention. After the mandatory period has ended, continued retention must be supported by another identifiable lawful basis, such as another statutory obligation or the necessity of preserving records for an ongoing legal claim. If no other lawful basis remains, the data must be deleted or destroyed in accordance with Articles 42–45 of the PDP Law. During mandatory retention, processing should also be restricted to the purpose that justifies the retention, and unnecessary further use should cease.

The available thesis materials do not conclusively establish whether these legal grounds and retention periods were communicated to the three users. The reviews report that users experienced difficulties obtaining explanations or solutions, but they do not include the complete privacy notice, the version of the consent screen presented during registration, the applicable terms and conditions, or UangMe's complete correspondence in response to the deletion requests. Consequently, the available evidence supports the finding that adequate communication has not been demonstrated, but it is insufficient to conclude definitively that no information was provided. A final assessment would require examination of the historical privacy policy, registration records, data-utilization consent, complaint correspondence, and the specific reasons given for refusing each request. Where a request is rejected as part of a consumer complaint, the rejection should be communicated to the user together with a clear reason, in accordance with OJK Regulation No. 22 of 2023.

If UangMe cannot demonstrate a valid legal basis for retaining particular data, or if it continues retaining the data after the relevant legal basis and retention period have ended, the continued processing may contravene Articles 16 and 20 of the PDP Law. The controller may then be required to terminate the processing and delete or destroy the data under Articles 42–45. The affected data subject may seek compensation under Article 12, while administrative sanctions may be imposed under Article 57, including a written warning, temporary suspension of processing, an order to delete or destroy the data, and an administrative fine. Civil liability may also arise where the requirements of an unlawful act, loss, fault, and causation are established. Criminal liability should only be considered where unlawful collection, disclosure, or use of personal data and the required element of intent can be proven; the user reviews alone are not sufficient to establish those elements.

Accordingly, the decisive issue is not merely whether personal data remained in UangMe's system after a rejected application or settled loan. The proper legal inquiry is whether UangMe can demonstrate a specific lawful basis, necessity and proportionality, a defined retention period, restriction of further use, adequate communication to users, and a reasoned response to each request. The three user reviews therefore indicate potential problems concerning transparency, data accuracy, deletion-request handling, and access to effective remedies, but additional evidence is required before a definitive finding of legal non-compliance can be made.

3.3 Legal Protection for Borrowers' Personal Data

Law Number 27 of 2022 provides the principal horizontal framework for personal-data protection. Its structure covers data-subject rights, lawful processing, controller and processor duties, data transfers, administrative sanctions, dispute resolution, prohibitions, and criminal provisions (UU RI, 2022). Applied to online lending, the law requires a provider to be able to justify why personal data are processed, ensure that processing is consistent with the stated purpose, maintain accuracy and security, and facilitate statutory rights under the conditions prescribed by law. The practical meaning is that a loan application cannot be treated as unlimited authorization to collect, retain, use, or disclose any information available from a user's device.

Financial-services regulation adds a sector-specific layer. Financial Services Authority Regulation Number 22 of 2023 requires financial-services businesses to protect the confidentiality and security of consumer data and frames collection conduct within consumer-protection norms(OJK, 2023). OJK's regulatory explanation emphasizes that collection should not use threats, violence, humiliating treatment, physical or verbal pressure, or communication directed to parties other than the consumer. Financial Services Authority Regulation Number 40 of 2024 provides the current sectoral framework for LPBBTI and places technology-based joint funding under updated licensing, governance, risk-mitigation, operational, and supervisory rules(OJK, 2024).

Consumer-protection law remains relevant because personal-data misuse can simultaneously constitute a violation of consumer rights to security, accurate information, fair treatment, and redress. Law Number 8 of 1999 therefore complements the PDP Law rather than being displaced by it(UU RI, 1999). The Electronic Information and Transactions framework also remains relevant to electronic

systems and the use of personal information in digital transactions. These overlapping statutes should be read systematically: the PDP Law supplies general data-governance duties, OJK rules add financial-sector conduct and supervision, consumer law protects transactional fairness and redress, and civil law provides a basis for damages where the requirements for liability are satisfied.

For UangMe users, preventive protection should operate before a dispute arises. The provider should use clear privacy notices, document the lawful basis for each processing purpose, minimize data collection, separate necessary permissions from optional ones, maintain accurate account records, and establish a transparent retention and deletion schedule. Rights requests should be handled through an auditable workflow with clear reasons when a request cannot lawfully be fulfilled. This approach reflects the preventive dimension of legal protection described by Hadjon, (1987): rights are most effectively protected when institutional and procedural safeguards reduce the probability of harm before coercive remedies are required.

Repressive protection becomes relevant after a suspected breach or misuse occurs. Consumers should have accessible complaint channels, evidence-preservation mechanisms, OJK complaint avenues, and judicial remedies where appropriate. A complaint system is not merely a service-quality feature; it is part of accountability because the ability to correct inaccurate data, stop improper processing, or obtain a reasoned response can determine whether statutory rights are meaningful in practice**.**

3.4 Provider Responsibility for Proven Personal Data Misuse

Legal responsibility must be assessed on the basis of proven conduct rather than platform reputation or complaint volume. If a provider unlawfully processes, discloses, retains, or fails to secure personal data, responsibility may arise under more than one legal regime. Administrative consequences can follow under personal-data and OJK regulation. Depending on the facts and statutory elements, other legal consequences may also apply. The existence of multiple regimes does not mean that sanctions are automatic or cumulative in every case; competent authorities must determine the applicable provision, evidence, and procedure.

Civil responsibility is particularly relevant when a borrower can demonstrate an unlawful act, fault or attributable conduct, loss, and a causal relationship. Article 1365 of the Indonesian Civil Code provides the general basis for compensation arising from an unlawful act. In an online-lending relationship, contractual duties may also shape the standard of conduct because the provider and borrower are bound by an electronic agreement that must be performed in good faith. A data-protection failure can therefore intersect with both statutory obligations and contractual expectations.

The thesis concludes that responsibility for misuse of personal information can include material and immaterial consequences, administrative measures, and civil compensation. That conclusion remains conceptually relevant, but its sectoral regulatory reference must be updated. The former POJK 10/2022 sanction structure cannot be presented as the current LPBBTI framework after the entry into force of POJK 40/2024. Current legal analysis should instead identify the sanctioning and supervisory mechanisms under the applicable 2024 LPBBTI rules, POJK 22/2023, and the PDP Law, while using POJK 10/2022 only to explain the historical development of the regulatory regime.

For the UangMe complaint patterns, responsibility would therefore depend on the evidence supporting each allegation. A deletion complaint requires examination of whether the data remain necessary under a lawful retention basis and whether the user received a valid explanation. A transparency complaint requires evidence of what terms changed, when notice was given, and what legal effect the change had. A collection complaint requires evidence of the communications, recipients, wording, frequency, and data disclosed. An inaccurate-account complaint requires audit records showing the contractual status and system history. This evidentiary approach prevents normative research from substituting allegation for proof while still identifying the provider's potential legal exposure.

3.5 Compliance Implications for Online Lending Providers

A practical compliance model can be derived from the analysis. First, data mapping should identify every item of personal data, its source, processing purpose, legal basis, recipient, retention period, and deletion trigger. Second, permission architecture should apply data minimization by default and avoid access that is not demonstrably necessary. Third, account and debt records should be synchronized across operational and collection systems to reduce inaccurate obligations. Fourth, collection workflows should technically restrict disclosure to unauthorized third parties and preserve audit logs. Fifth, rights requests and complaints should have measurable service standards,

escalation paths, and written reasons for decisions. Sixth, periodic compliance audits should test both legal documentation and actual system behavior.

This model also clarifies the relationship between regulation and trust. Consumer trust does not arise solely from an OJK license or a privacy policy; it is produced by consistent system behavior that allows users to understand, verify, challenge, and, where legally permitted, terminate the processing of their data. The complaint patterns documented in the thesis indicate that perceived loss of control over data is itself a significant harm to trust. Strengthening accountability mechanisms is therefore both a legal requirement and a condition for sustainable digital lending.

4. CONCLUSION

Indonesian law provides a substantial multi-layered basis for protecting personal data in online lending through the PDP Law, consumer-protection law, electronic-transaction law, OJK consumer-protection regulation, and the current LPBBTI framework under POJK 40/2024. In the UangMe case materials, the principal legal-risk indicators concern data deletion and retention, proportionality of data access, transparency of policy changes, use of information in collection, accuracy of account obligations, and effectiveness of complaint handling. These indicators do not establish that UangMe committed a violation; they identify factual questions that must be tested against statutory duties and evidence. If misuse is proven, responsibility may arise through administrative measures, civil compensation, and other consequences provided by applicable law. The most important practical implication is that legal protection should be embedded in the data life cycle through minimization, transparent purposes, accurate records, secure processing, auditable deletion, responsible collection, and responsive complaint mechanisms. Future research should test these normative findings against regulator decisions, court judgments, platform audit evidence, and direct consumer interviews so that the effectiveness of the post-2024 LPBBTI framework can be evaluated empirically.

REFERENCES

Angeline, P., & Dwijayanthi, P. T. (2023). Perlindungan data pribadi bagi penerima dana fintech lending dalam perspektif hukum positif Indonesia. Kertha Semaya: Journal Ilmu Hukum, 11(12), 2996–3007. https://doi.org/10.24843/KS.2023.v11.i12.p19

Apiatna, D. S. (2025). Review of the UangMe application. In Google Play Store.

Hadjon, P. M. (1987). Perlindungan hukum bagi rakyat di Indonesia: Sebuah studi tentang prinsip-prinsipnya, penanganannya oleh pengadilan dalam lingkungan peradilan umum dan pembentukan peradilan administrasi negara. Bina Ilmu.

Novelin, T., Rusmana, I. P. E., & Sukmayanti, M. S. (2025). Melindungi data pribadi: Tantangan dan upaya hukum dalam fintech lending. Kertha Semaya: Journal Ilmu Hukum, 13(5), 1004–1017. https://doi.org/10.24843/KS.2025.v13.i05.p18

OJK. (2023). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

OJK. (2024). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.

Parikesit, A. (2025). Review of the UangMe application. In Google Play Store.

Priambono, L., Sudirman, & Umar, W. (2024). Kebocoran data pribadi akibat penagihan utang pinjaman online ilegal. UNES Law Review, 6(4), 11238–11243. https://doi.org/10.31933/unesrev.v6i4.2068

Rahmawati, E., Huda, M., & Aldhi, I. F. (2024). Personal data misuse in fintech lending providers from perspective Indonesian cyberlaw. Airlangga Development Journal, 8(1), 8–20. https://doi.org/10.20473/adj.v8i1.56398

Rohendi, A., & Kharisma, D. B. (2024). Personal data protection in fintech: A case study from Indonesia. Journal of Infrastructure, Policy and Development, 8(7), 4158. https://doi.org/10.24294/jipd.v8i7.4158

Syahruddin, N. I., & Zulfa, E. A. (2024). Personal data protection violations by fintech lending in Indonesia. Journal of Law, Politic and Humanities, 4(4), 999–1006. https://doi.org/10.38035/jlph.v4i4.414

UU RI. (1999). Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

UU RI. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

UU RI. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Widianingsih, W. (2025). Review of the UangMe application. In Google Play Store.