JOURNAL OF GOVERNANCE AND LAW REFORM
YEARS 2026, VOLUME 01, NUMBER 01
DOI: https://doi.org/10.64670/jglr.v1i1.62

CATALIST JOURNAL
PUBLISHERS

RESEARCH ARTICLE

Protection Of Third Party Personal Data When Using Emergency Contacts On The Shopee Paylater Service

Elmo Septian Rasyid[1], Ainun Nabilah[2], Cahya Utami Aldana[3] , Miranti[4], Andriyanto Adhi Nugroho[5]
[12345]Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia

ABSTRACT

This research examines the protection of third-party personal data in the practice of providing emergency contact information within Buy Now Pay Later services, particularly Shopee PayLater, where such data is often included without the consent of its actual owner. This situation raises significant legal concerns because third parties, who have no contractual relationship with the service provider, nonetheless become subjects of data processing and debt collection activities. The study employs a normative juridical method by analyzing the Personal Data Protection Law, the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019, sectoral regulations issued by the Financial Services Authority, and relevant judicial decisions including the Central Jakarta District Court Decision Number 689 Pdt G 2021 and the Supreme Court Decision Number 1206 K Pdt 2024. Using the right to privacy theory and consent theory, the findings show that processing third-party data without direct and explicit consent contradicts fundamental principles of personal data protection and violates individual privacy rights. The research further reveals that Indonesia's current legal framework does not provide a comprehensive mechanism for third-party consent, resulting in regulatory gaps related to data collection, consent verification, and limitations on the use of third-party information in digital financial services. This study concludes that existing regulations do not provide adequate protection for third parties and highlights the need for more detailed legal provisions governing the collection, verification, and restricted use of emergency contact data within Buy Now Pay Later services.

ARTICLE HISTORY :
Received : 20 December 2025
Revised : 25 January 2026
Accepted : 28 January 2026

KEYWORDS :
Personal Data; Protection; Third Party Consent; Emergency Contact; Shopee PayLater;

CORRESPONDENCE :
Nama: Ainun Nabilah
Email: ainunnabilah34@gmail.com

1. Introduction

The development of digital financial services in recent years has shown rapid growth, particularly in Buy Now Pay Later (BNPL) financing models, such as Shopee PayLater. This scheme offers easy access to credit without complicated procedures, making it attractive to groups of people who previously had difficulty accessing conventional financial services (Pertiwi & Hariyana, 2025). However, behind this convenience, serious issues have emerged regarding personal data protection, especially for parties not directly involved in legal relationships. One of the most prominent issues is the practice of listing emergency contacts without the owner's consent. In many cases, users list the phone numbers of family, colleagues, or friends to fulfill administrative requirements when registering for services, without notification or requesting their consent. When payments are late, these third parties become targets of collection efforts, which may include text messages, repeated calls, and even intimidation from debt collectors (Muzakkir, 2025).

This phenomenon demonstrates that legal relationships on digital platforms involve not only service providers and users, but also other parties without a direct contractual relationship. Users are in a weak position due to their dependence on the service, while third parties are most vulnerable because they lack control over the inclusion of their data, but still bear the psychological burden. Service providers are in a dominant position because they control the processing and use of data (Situmorang, 2023). This imbalance highlights regulatory gaps in personal data protection mechanisms, particularly regarding the

validity of consent for the use of third-party data, which is not yet regulated in detail in national law (Martadikusuma, 2025).

The issue of personal data misuse in the fintech sector has received considerable legal attention. Central Jakarta District Court Decision No. 689/Pdt.G/2021 confirmed that online lending applications can access users' personal data, including contact lists and call histories, without a transparent consent mechanism (Syaiful & Sugiyono, 2024). This data dissemination impacts third parties who never consented to or were aware of the use of their data, often making them targets for collection and psychological pressure. Similar considerations emerged in Supreme Court Decision No. 1206 K/Pdt/2024, which emphasized that the practice of disseminating and using personal data without a legal basis, including against third parties, constitutes a serious violation requiring more decisive regulatory intervention. This phenomenon demonstrates the need for more precise third-party consent mechanisms. Existing regulations, both the PDP Law and sectoral regulations, primarily focus on the relationship between electronic system providers and primary users and do not explicitly regulate the use of third-party data. As a result, service providers are in a dominant position, while third parties lack the legal capacity to refuse or control the use of their data (Rohendi & Kharisma, 2024).

This research, using the theory of privacy rights, asserts that every individual has the right to control their personal information, so data such as telephone numbers should not be used without the owner's consent. In the context of Shopee PayLater, third parties listed as emergency contacts experience a violation of their privacy rights when their data is used for verification or billing without consent. Meanwhile, the Consent Theory asserts that data processing is only lawful if consent is given by the data owner freely, consciously, specifically, and informed. Because Shopee PayLater only obtains consent from the primary user, the processing of third-party data lacks a valid legal basis. These two theories together strengthen the argument that listing emergency contacts without consent violates the fundamental principle of personal data protection for both the primary user and the third party (Post, 2017). Previous research has shown that the misuse of personal data by fintech services is structural, with many fintech applications automatically accessing contact lists without valid written consent (Stewart & Jürjens, 2018), Other studies emphasize the weak implementation of data protection regulations, resulting in frequent unauthorized data dissemination (Aldboush & Ferdous, 2023). However, previous research generally focuses on direct users and has not explicitly addressed the misuse of third-party data, such as emergency contacts. Therefore, this study is essential in addressing this gap in the literature.

Based on this description, the protection of third-party personal data in the use of emergency contacts is a crucial issue that has not received adequate attention. Research on the responsibilities of digital service providers, particularly Shopee PayLater, is relevant for addressing this legal gap and providing an academic basis for formulating more comprehensive policies. The research questions are formulated as follows: (1) How do Indonesian positive legal regulations regulate the use and processing of personal data in the listing of emergency contacts on the Shopee PayLater service, and (2) How do legal provisions regulate the consent mechanism, and do these regulations cover the protection of third-party personal data in the Buy Now Pay Later service.

2. Methodology

This research uses a normative juridical method, an approach that focuses on the analysis of legal norms within the Indonesian legal system. This method was chosen because the research problem formulation focuses on how positive law regulates the use and processing of personal data in the inclusion of emergency contacts in digital financial services, specifically Buy Now Pay Later services such as Shopee PayLater, as well as how consent mechanisms and third-party data protection are regulated. The normative approach is considered most appropriate because this research emphasizes the analysis of legal rules, principles, doctrines, and court decisions, rather than empirical facts on the ground. Thus,

this study aims to assess the applicability and relevance of legal norms in the context of personal data misuse in fintech services (Hamzani et al., 2023).

The primary data sources used include the Personal Data Protection Law, the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and the Financial Services Authority (OJK) regulations regarding fintech services, plus court decisions such as Central Jakarta District Court Decision No. 689/Pdt.G/2021 and Supreme Court Decision No. 1206 K/Pdt/2024. Furthermore, secondary legal materials, including academic literature, books, and legal journals, were utilized to enhance the analysis, focusing on consent, third-party consent, privacy rights, and principles of personal data protection. Tertiary legal materials, including legal dictionaries, encyclopedias, and news articles on the inclusion of emergency contacts without consent, were also utilized to enrich conceptual understanding, while maintaining the normative and systematic nature of the research (Tikkinen-Piri & Markkula, 2018).

3. Results and discussion

3.1 Positive legal regulations in Indonesia regarding the use of personal data in the inclusion of emergency contacts on the Shopee PayLater service.

Indonesia has a fairly comprehensive legal framework governing personal data protection through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law contains a fairly broad definition of personal data, namely "data about an identified or identifiable natural person, either directly or indirectly," thus encompassing any form of information that can be linked to a person's identity, including personal telephone numbers (Rosadi & Aisy, 2023). Under this definition, the telephone number listed as an emergency contact in the Shopee PayLater service essentially constitutes personal data if it can lead to the identification of a specific individual, namely a third party selected by the service user. Article 16 of the Personal Data Protection Law explains that personal data processing activities are not limited to data collection but also encompass a range of activities such as storage, use, distribution, and destruction. Therefore, when a PayLater user lists a third party's number as an emergency contact, this action falls under the category of "personal data collection." Meanwhile, when service providers like Shopee PayLater store, verify, or even use these numbers for billing purposes, this fulfills the elements of "personal data processing" as defined in the Personal Data Protection Law.

Therefore, any processing of personal data, including third-party data, must comply with the basic principles of personal data protection, namely the existence of a legitimate basis for processing such data, one of which is the express consent of the data owner. However, in practice, the inclusion of emergency contacts in BNPL services is often based only on the consent of the primary user, not the owner of the number used as the emergency contact. This is where a significant legal issue arises: can the processing of third-party data by a service provider be considered lawful if consent is not given directly by the data owner. Applicable regulations do not provide a clear answer, but the general principle of the Personal Data Protection Law emphasizes that consent must come from the personal data owner themselves. In this context, the legal vacuum arises. The Personal Data Protection Law does not explicitly regulate how the consent mechanism should be implemented when the personal data being processed does not belong to the user, but to a third party listed as an emergency contact. However, normatively, every individual has the full right to control the processing of their personal data, as affirmed in Article 5 of the Personal Data Protection Law concerning the rights of personal data subjects, including the right to know, give consent, or object to the processing of their personal data. Without clear regulations, the practice of listing emergency contacts has the potential to conflict with the principles of personal data protection formally established in Indonesian law.

In addition to the Personal Data Protection Law, more technical provisions regarding the use of personal data in digital financial services are also contained in sectoral regulations of the Financial Services Authority (OJK). One necessary provision is OJK Circular Letter Number 19/SEOJK.06/2023 concerning the Provision of Information Technology-Based Joint Funding Services. This regulation

emphasizes that emergency contacts should not be targeted for debt collection, given that parties listed as emergency contacts are not contractually bound to the service provider. This provision clearly demonstrates that the Financial Services Authority (OJK) views third-party data as an entity that must be protected, and therefore, its use in the collection process cannot be done freely or without limits. Thus, although this regulation is not specifically designed to regulate BNPL (Buy Now, Pay Later) services like Shopee PayLater, its principles remain relevant as they both relate to third-party data collection practices in digital financial services.

This creates a positive legal gap regarding how third-party data is obtained, how data owner consent must be granted, and the extent to which service providers are authorized to process such data. To date, there are no digital financial sector regulations that explicitly govern procedures for recording emergency contacts, verifying the number owner's consent, or protecting third-party personal data from the collection stage. The prohibition on emergency contact billing, as stipulated in OJK Circular Letter No. 19/SEOJK.06/2023, only limits the billing stage and does not address the upstream aspect, namely the collection and processing of third-party data by digital platforms. This gap in norms creates legal uncertainty, both for service providers like Shopee PayLater and for third parties whose data is processed without a precise consent mechanism. It also demonstrates that Indonesia's positive legal framework is not yet fully comprehensive in regulating personal data processing in the context of emergency contact recording.

3.2 Regulations and legal provisions governing the consent mechanism regarding the scope of third-party personal data protection in Buy Now Pay Later services.

Within Indonesia's positive legal framework, the consent mechanism is a key pillar in the processing of personal data. This is expressly stated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), specifically Article 20 paragraph (2), which states that one of the legal bases for data processing is "the explicit and valid consent of the personal data subject." This provision demonstrates that consent is not merely an administrative formality, but rather the legal basis that determines the legitimacy of all data processing activities, including the collection, storage, use, and dissemination of data. Therefore, every form of personal data processing, whether by digital financial service providers such as BNPL or by other parties, must have apparent legal legitimacy through this consent mechanism (Rahman, 2025).

Furthermore, provisions regarding consent in data processing are also strengthened through secondary legal sources. A legal article published by Hukumonline explains that consent can be given in writing or recorded, provided it is given freely, specifically, based on sufficient information, and without coercion. In the context of Buy Now, Pay Later services like Shopee PayLater, this principle is crucial because service providers are required to ensure that users' consent to the processing of their own personal data and the data of others they provide is given consciously and through a transparent mechanism. This requirement aims to protect the rights of data subjects and prevent misuse of personal data. Several leading law firms, such as ABNR, also emphasize that the concept of consent in the Personal Data Protection Law must be understood as verifiable consent, meaning that providers must be able to prove that the consent was actually given by the personal data owner. Thus, the Personal Data Protection Law not only emphasizes the obligation to obtain consent but also requires providers to maintain evidence that such consent was validly given. This has important implications for the use of third-party personal data as emergency contacts in BNPL services, as consent must come not only from the primary user but also from the owner of the listed telephone number.

In the context of BNPL services like Shopee PayLater, the issue of consent becomes more complex because the data subject is not only the user but also the third party whose number is listed as an emergency contact. The PDP Law establishes fundamental data subject rights, including the right to give consent, withdraw consent, obtain access, and obtain information regarding the processing of personal

data. This provision emphasizes that every individual has control over their personal data and that processing may only occur if there is a valid legal basis. This regulation should provide protection for third parties whose data is entered into the Shopee PayLater system without their direct consent. However, in practice, this provision still leaves considerable room for interpretation, particularly when there is no validation mechanism to determine whether the phone number owner's consent has been obtained before processing begins.

This legal gap is evident in the absence of explicit provisions on third-party consent verification procedures. Existing regulations only stipulate that consent must be granted by the personal data owner, but do not specify how such consent must be obtained when an emergency contact is listed by another user in a digital financial application. There are no provisions requiring service providers to confirm to third parties that their data will be used, nor do they provide a mechanism for third parties to consent to or decline such processing from the outset. As a result, third parties without a contractual relationship with Shopee PayLater remain subject to data processing to which they may not have consented. This situation highlights that while consent mechanisms are fundamentally regulated in the PDP Law, this norm has not been specifically applied in the context of emergency contacts in BNPL services, resulting in suboptimal legal protection for third-party personal data. Therefore, regarding Buy Now, Pay Later services like Shopee PayLater, Indonesia's positive legal framework actually establishes strict basic principles regarding consent, although it does not explicitly regulate the mechanism for third-party consent. However, the provisions of the Personal Data Protection Law and expert opinion clearly state that consent must come from the personal data subject themselves, not from unauthorized third parties. Therefore, listing emergency contacts without the number owner's permission is inconsistent with the basic principles of personal data protection in the Personal Data Protection Law.

4. Conclusion

Based on Indonesian positive law, it can be concluded that personal data protection is fundamentally grounded in the Personal Data Protection Law, the Electronic Information and Transactions (ITE) Law, Government Regulation 71/2019, and sectoral provisions such as the Financial Services Authority Regulation (POJK) and the Financial Services Authority Circular Letter (SEOJK), which expressly prohibit billing of emergency contacts. This legal framework demonstrates that Indonesia has established general principles regarding data subject rights, data controller obligations, and limitations on personal data processing in digital financial services. However, when specifically linked to the practice of including emergency contacts in BNPL services like Shopee PayLater, the existing regulations still leave significant normative gaps.

To date, there are no explicit regulations governing how third-party data is obtained, whether data owner consent is required, and how service providers are obligated to process and protect such data. The prohibition on billing of emergency contacts only governs the final stage of data use, while the upstream process, from collecting and validating consent to storing third-party data, remains incompletely regulated. As a result, the inclusion of emergency contact information by users and the processing of third-party numbers by service providers operate within an unclear legal framework. Therefore, while Indonesian law provides a general framework for personal data protection, specific regulations governing the use and processing of third-party personal data for emergency contact information on the Shopee PayLater service remain inadequate. This situation highlights the need for stronger and more detailed regulations to ensure legal certainty for both third parties and service providers.

Indonesian law already regulates consent as the basis for processing personal data and establishes data subject rights. However, these regulations do not explicitly address third-party consent mechanisms when third-party data is included in BNPL services. Thus, there is a regulatory gap that could undermine

the effectiveness of third-party personal data protection when quoting emergency contact information in digital financial services. The regulations outline the basis for consent for the processing of personal data, but do not specifically address third-party consent mechanisms in the context of emergency contacts. As a result, BNPL providers like Shopee PayLater are in a position where they can collect third-party data without regulations requiring verification of that party's consent. This lack of regulation poses a risk that third-party personal data protection rights will be less secure, even though PDP regulations generally apply.

5. Bibliography

Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies*.

Hamzani, A. I., Widyastuti, T. V., Khasanah, N., & Rusli, M. H. M. (2023). Legal Research Method: Theoretical and Implementative Review. *International Journal of Membrane Science and Technology*, *10*(2), 3610–3619. https://doi.org/10.15379/ijmst.v10i2.3191

Martadikusuma, A. D. (2025). *Perlindungan Hukum Bagi Konsumen Dalam Transaski Buy Now Pay Later (BNPL) di Indonesia: Tinjauan Regulasi dan Praktik Bisnis*. https://doi.org/https://doi.org/10.61104/alz.v3i2.1062

Muzakkir, M. (2025). *Integration of Fintech Services in E-Commerce Platforms: Case Study of Paylater Usage in Generation Z*. https://doi.org/https://doi.org/10.37673/jebi.v10i1.6094

Pertiwi, T. K., Joseph, C., Warmana, G. O., Khoirotunnisa, F., & Hariyana, N. (2025). Exploring Platform Trust, Borrowing Intention, and Actual Use of PayLater Services in Indonesia and Malaysia. *Journal of Risk and Financial Management*.

Post, R. C. (2017). *Rereading Warren and Brandeis: Privacy, property, and appropriation. In Privacy (pp.*

Rahman, F. (2025). *Safeguarding personal data in the public sector: Unveiling the impact of the new Personal Data Protection Act in Indonesia. UUM Journal of Legal Studies, 16(1), 1-18.*

Rohendi, A., & Kharisma, D. B. (2024). Personal data protection in fintech: A case study from Indonesia. *Journal of Infrastructure, Policy and Development*.

Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). (2023). *Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?. International Review of Law, Computers & Technology, 37(1), 78-90.*

Situmorang, S. H. (2023). *Mobile Payment: Trends in the Digital Shopping Behaviour of the Millennial Generation. In Digital Transformation for Business and Society (pp. 196-217). Routledge.*

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*, *26*(1), 109–128.

Syaiful, R. D., & Sugiyono, H. (2024). (2024). *Misuse of Consumer Personal Data Through Illegal Fintech Peer To Peer Lending. Justisi, 10(1),* (pp. 189–201).

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). *EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.*