RECHTSVINDING
Vol. 4, 2 (July-December, 2026), pp. 19-26
EISSN: 2987-4424, DOI: https://doi.org/10.59525/rechtsvinding.1856

Platform Liability as a Personal Data Controller for The Processing of Emergency Contact Data in Fintech Lending Agreements (A Study on The Kredit Pintar Platform)

Raka Haikal Anfasya[1], Andriyanto Adhi Nugroho[1], Iwan Erar Joesoef[1]

[1] Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia

ARTICLE INFO

Keywords:

Fintech Lending;
Emergency Contact;
Personal Data Protection;
Personal Data Controller;
Platform Liability

Article history:

Received 2025-05-01
Revised 2026-06-04
Accepted 2026-07-09

ABSTRACT

The development of financial technology lending (fintech lending) drives service providers to collect and process users' personal data, including the personal data of emergency contacts as part of loan application requirements. In practice, the processing of emergency contact personal data is conducted based on standard clauses that require users to state that they have obtained consent from the party registered as an emergency contact and transfer certain liabilities to the user. This condition raises issues regarding the validity of personal data processing and the platform's liability as a Personal Data Controller under Law Number 27 of 2022 concerning Personal Data Protection. This research aims to analyze the validity of the processing of emergency contact personal data in the fintech lending agreement of the Kredit Pintar Platform based on Law Number 27 of 2022 concerning Personal Data Protection and to analyze the platform's liability as a Personal Data Controller for the processing of emergency contact personal data. This research utilizes a normative legal research method with a statute approach, a conceptual approach, and a contract study approach. Legal materials were obtained through a literature study and analyzed qualitatively using a prescriptive method. The results of the research indicate that the validity of processing emergency contact personal data is insufficient if it is merely based on the user's statement of having obtained consent from the emergency contact, but must satisfy a lawful basis for processing as well as the principles of personal data protection as regulated in the Personal Data Protection Law. Furthermore, the platform as a Personal Data Controller retains legal liability for the processing of emergency contact personal data; thus, clauses transferring liability to the user do not eliminate the platform's legal obligations to protect the rights of the Personal Data Subject.

Corresponding Author:
Raka Haikal Anfasya
Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia; 2410622029@mahasiswa.upnvj.ac.id

1. INTRODUCTION

The development of information technology has driven the transformation of the financial services sector through the implementation of Information Technology-Based Joint Funding Services (*Layanan Pendanaan Bersama Berbasis Teknologi Informasi* / LPBBTI) or financial technology lending (fintech lending) (Otniel Yustisia Kristian, 2022). The utilization of digital technology enables the processes of application, approval, up to loan disbursement to be executed electronically through digital platforms. This innovation provides convenience, efficiency, and expansion of financing access for the public, yet at the same time, it also generates various legal consequences, particularly relating to the legal relationships of the parties and data management in the operation of information technology-based services. The implementation of fintech lending cannot be separated from personal data processing activities as part of digital service operations. In the loan application process, providers perform the collection, storage, use, and disclosure of users' personal data for the purposes of identity verification, creditworthiness analysis, and risk mitigation. Given the importance of protecting personal data, Article 28G paragraph (1) of the 1945 Constitution of the State of the Republic of Indonesia guarantees everyone's right to personal protection. This constitutional guarantee was subsequently manifested through Law Number 27 of 2022 concerning Personal Data Protection, which regulates that any processing of personal data must be conducted based on a lawful basis for processing, respect the rights of personal data subjects, and implement the principle of accountability at every stage of data processing (Gita Theresa, 2024).

One form of personal data processing in the operation of fintech lending is the collection of emergency contact data, which generally encompasses names, telephone numbers, and relationships with the user. The existence of an emergency contact is fundamentally intended as a means of communication if the provider experiences difficulty contacting the user, as well as part of risk mitigation efforts in the implementation of funding services. Nevertheless, the processing of emergency contact data creates legal issues because the data being processed belongs not only to the user as a party to the agreement, but also to a third party who has no direct contractual relationship with the fintech lending provider. Legal problems arise because the emergency contact is not a party to the legal relationship between the fintech lending provider and the user, yet their personal data remains an object of processing by the provider. As personal data subjects, emergency contacts in principle possess the right to the protection of their personal data as guaranteed under Law Number 27 of 2022 concerning Personal Data Protection (Kinanti, Ramadhani, & Wiraguna, 2025). Therefore, the processing of emergency contact personal data must have a valid legal basis and must be carried out while still respecting the rights of the personal data subject. The issue is that in the practice of operating fintech lending, consent to the use of emergency contact data is generally only declared by the user as the borrower, thereby raising questions as to whether such a declaration has fulfilled the principles of personal data protection and is sufficient to serve as a basis for the provider to process personal data belonging to a third party (Aprillia Mieke U., 2025).

This issue is reflected in Article 3.11 of the Terms and Conditions (*Syarat dan Ketentuan*) of the Kredit Pintar Platform, which essentially regulates that the user guarantees they have obtained consent from the party registered as an emergency contact and releases and holds harmless the provider from any losses, claims, or legal lawsuits arising in connection with communications made to the said emergency contact. On the other hand, the Privacy Policy (*Kebijakan Privasi*) of the Kredit Pintar Platform states that personal data processing is carried out based on consent and in accordance with the provisions of the applicable laws and regulations. These provisions raise questions as to whether the provider, as a Personal Data Controller, can fully rely on the unilateral declaration of the user as the basis for processing the personal data of the emergency contact, or whether they retain a legal obligation to ensure that such consent is genuinely given by the owner of the personal data (Kredit Pintar, 2026).

This condition gives rise to problems regarding the limits of the provider's liability as a Personal Data Controller in processing emergency contact data. Law Number 27 of 2022 concerning Personal Data Protection in principle stipulates that every instance of personal data processing must be conducted based on a lawful basis for processing and obligates Personal Data Controllers to protect the rights of personal data subjects. On the other hand, Article 1338 paragraph (3) of the Indonesian Civil Code requires that

every agreement be executed in good faith, while Article 18 of Law Number 8 of 1999 concerning Consumer Protection in principle prohibits business actors from including standard clauses that shift liability to consumers (Fajar Nugroho Handayani, 2020). Therefore, it is necessary to examine whether the clause regarding emergency contacts in fintech lending agreements aligns with the principles of personal data protection, good faith in contract law, and consumer protection in Indonesia. This problem is analyzed using the Theory of Legal Protection propounded by Philipus M. Hadjon. According to Hadjon, legal protection constitutes an effort to safeguard public rights through both preventive and repressive protection. Preventive legal protection aims to prevent violations of rights through regulations that provide certainty regarding the rights and obligations of the parties before a dispute arises, whereas repressive legal protection is provided through dispute resolution mechanisms once a violation of rights has occurred. In the context of this research, the theory is utilized to analyze whether the mechanism for processing emergency contact personal data, including the basis of consent and the allocation of liability within the fintech lending agreement, has provided adequate legal protection for the emergency contact as a personal data subject (Daffa Arya Prayoga, Jadmiko Anom Husodo, & Andiana Elok Puri Maharani, 2023).

Research regarding personal data protection in the operation of fintech lending generally focuses more on the protection of the user's personal data as a debtor, electronic system security, or consumer protection against standard clauses in electronic agreements. Meanwhile, studies concerning the platform's liability for the processing of emergency contact personal data as a third party who is not a party to the loan agreement remain relatively limited. Yet, an emergency contact is a personal data subject whose rights must still be protected despite not having a direct contractual relationship with the provider. Therefore, this research attempts to fill this academic gap by analyzing the platform's liability as a Personal Data Controller in the processing of emergency contact personal data based on the legal provisions applicable in Indonesia.

Based on the aforementioned description, this research is crucial to be conducted in order to examine the platform's liability as a Personal Data Controller in the processing of emergency contact personal data within fintech lending services. This research will analyze the compatibility of the clause regarding emergency contacts in the Terms and Conditions as well as the Privacy Policy of the Kredit Pintar Platform with the provisions of Law Number 27 of 2022 concerning Personal Data Protection, the Indonesian Civil Code, and Law Number 8 of 1999 concerning Consumer Protection. The results of the research are expected to contribute to the development of legal science, particularly in the fields of personal data protection law and contract law, as well as to serve as recommendations for fintech lending providers in drafting contractual clauses and privacy policies that provide legal certainty and balanced protection for all stakeholders involved.

2. METHODS

The research method used in this study is normative legal research featuring a statute approach, a conceptual approach, and a contract study approach (Marzuki, 2021). The statute approach is used to examine the provisions of laws and regulations related to personal data protection, agreements, consumer protection, and the implementation of financial technology lending (fintech lending), including, among others, the Indonesian Civil Code, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 8 of 1999 concerning Consumer Protection, Financial Services Authority Regulation Number 40 of 2024 concerning Information Technology-Based Joint Funding Services, as well as other laws and regulations relevant to the object of research. The conceptual approach is utilized to analyze the concepts of Personal Data Controller liability, the lawful basis for personal data processing, consent, and legal protection for personal data subjects as a foundation for analyzing the legal standing of emergency contacts in fintech lending services (Natasya Klarisa Paruntu & Amad Sudiro, 2025). Meanwhile, the contract study approach is employed to review and analyze the clauses concerning emergency contacts in the Terms of Service and Privacy Policy of the Kredit Pintar Platform, specifically the provisions governing consent for personal data processing and the imposition of liability for the use of emergency

contact data. Primary legal materials in this research consist of laws and regulations relating to personal data protection, consumer protection, contract law, and the operation of fintech lending. Secondary legal materials were obtained from books, scientific journals, previous research results, doctrines, and legal literature relevant to the themes of personal data protection, legal liability, contract law, and fintech lending. This research also utilizes the Terms of Service and Privacy Policy of the Kredit Pintar Platform as legal materials that serve as the objects of analysis. Legal materials were analyzed qualitatively using a prescriptive method, namely through an analysis of the provisions of laws and regulations, doctrines, legal theories, and contractual clauses to derive legal arguments regarding the platform's liability as a Personal Data Controller in the processing of emergency contact personal data within fintech lending services, as well as to formulate recommendations for the application of clauses that align with the principles of personal data protection and provide legal certainty for the parties.

3. FINDINGS AND DISCUSSION

Validity of The Processing of Emergency Contact Personal Data in Fintech Lending Agreements Based on Law Number 27 of 2022 concerning Personal Data Protection

In the operation of financial technology lending (fintech lending), providers generally obligate users to include an emergency contact as one of the prerequisites in the loan application process. The requested information generally takes the form of a name, telephone number, and the relationship between the emergency contact and the user (Pranoto, 2025). The existence of an emergency contact is intended as a means of communication if the provider experiences difficulty contacting the user, as well as part of risk mitigation efforts in the operation of funding services. Nonetheless, an emergency contact is inherently neither a debtor, a creditor, nor a guarantor within the financing legal relationship, but rather a third party whose personal data is processed by the provider without becoming a party to the loan agreement.

As a third party whose personal data is processed by the provider, an emergency contact is in principle a Personal Data Subject as referred to in Article 1 number 9 of Law Number 27 of 2022 concerning Personal Data Protection. Meanwhile, information in the form of a name and telephone number collected by the provider is categorized under Personal Data as regulated in Article 1 number 1 of Law Number 27 of 2022 concerning Personal Data Protection (Dadan Kurniawan, 2026). Therefore, the emergency contact is entitled to obtain legal protection over their personal data even though they do not possess a direct contractual relationship with the provider. In line with the Theory of Legal Protection put forward by Philipus M. Hadjon, preventive legal protection is manifested through regulations that guarantee the rights of legal subjects prior to the occurrence of a violation. In the context of personal data processing, such protection is realized through the obligation of the Personal Data Controller to ensure that every data processing instance is performed based on a valid legal basis and respects the rights of personal data subjects in compliance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection (Hadjon, 1987).

As a form of preventive legal protection for personal data subjects, Law Number 27 of 2022 concerning Personal Data Protection regulates that every processing of personal data must be grounded on a lawful basis for processing. This provision is set forth in Article 20 paragraph (1), which determines that personal data processing may be carried out if it fulfills one of the processing bases regulated under the law, including, among others:

- Based on the valid consent of the Personal Data Subject for one or several specific purposes;
- The performance of an agreement;
- The fulfillment of a legal obligation;
- The protection of vital interests of the personal data subject;
- The execution of tasks in the framework of public interest; or
- The fulfillment of a legitimate interest while continuing to observe the objectives, necessities, and balance of interests between the Personal Data Controller and the rights of the Personal Data Subject.

Consequently, the validity of personal data processing is not merely determined by the existence of the processing itself, but rather by the fulfillment of a lawful basis for processing as specified in the Personal Data Protection Law (Republik Indonesia, 2022).

When linked to the provisions of Article 20 of Law Number 27 of 2022 concerning Personal Data Protection, the basis for processing emergency contact personal data utilized by the Kredit Pintar Platform essentially relies on consent. This is reflected in Article 3.11 of the Terms of Service, which states that the user guarantees they have obtained consent from the party registered as an emergency contact. Thus, the provider bases the validity of processing the emergency contact's personal data on the user's declaration that such consent has been granted by the owner of the personal data. Nevertheless, the said clause does not regulate the mechanism utilized by the provider to ensure that the consent is truly given consciously, voluntarily, and by the personal data subject concerned. This condition raises questions as to whether a unilateral declaration from the user is sufficient to satisfy the lawful basis requirements for processing as regulated in the Personal Data Protection Law.

From the perspective of preventive legal protection, the fulfillment of the basis for processing personal data is insufficient if it is merely based on the existence of a statement in a contractual clause, but it must also be actualized through a mechanism capable of guaranteeing the fulfillment of the rights of the Personal Data Subject (Tegar Uji Asetko Runto, Tahasak Sahay, & Andika Wijaya, 2026). Consequently, the clause of Article 3.11 of the Terms of Service of the Kredit Pintar Platform, which bases the processing of emergency contact personal data on guarantees from the user, has not yet fully demonstrated how the provider ensures that such consent is genuinely given by the owner of the personal data. Yet, as a Personal Data Controller, the provider remains obligated to apply the principles of prudence, transparency, and accountability at every stage of personal data processing (Jebaru & Widiatno, 2026). Accordingly, the validity of processing emergency contact personal data is determined not only by the existence of a unilateral declaration from the user, but also by the fulfillment of the principles of personal data protection as regulated under Law Number 27 of 2022 concerning Personal Data Protection (Muhammad Faiq Nizam, 2026).

Based on the aforementioned explanation, the validity of processing emergency contact personal data in fintech lending agreements is determined not only by the existence of a clause stating that the user has obtained consent from the emergency contact, but also by the fulfillment of a lawful basis for processing as regulated under Law Number 27 of 2022 concerning Personal Data Protection. Reviewed from the perspective of preventive legal protection, the provider as a Personal Data Controller retains a legal obligation to ensure that personal data processing is carried out in accordance with the principles of legality, transparency, accountability, and respect for the rights of the Personal Data Subject. Therefore, the use of a clause that solely bases processing on the user's declaration is insufficient to guarantee the fulfillment of legal protection for the emergency contact as a third party. A more adequate mechanism is required to ensure that the basis for personal data processing has truly been fulfilled in accordance with the provisions of the Personal Data Protection Law.

Platform Liability as A Personal Data Controller for The Processing of Emergency Contact Personal Data in Fintech Lending Agreements

The validity of personal data processing as expounded in the preceding section serves as the fundamental basis for determining the legal liability of fintech lending providers. Under Law Number 27 of 2022 concerning Personal Data Protection, the party that determines the purposes of and conducts the processing of personal data is designated as a Personal Data Controller, thereby giving rise to an inherent legal obligation to ensure that the entirety of the data processing operations is carried out in conformity with the provisions of the laws and regulations. Consequently, a fintech lending provider acts not merely as a provider of information technology-based loan services, but also as a legal subject bearable of liability for any personal data processing activities, including the personal data of emergency contacts acquired during the loan application process (Doni Harianto, Adithia Permana Sinaga, & Fajriansyah, 2025).

Viewed from the Theory of Legal Protection propounded by Philipus M. Hadjon, legal protection is manifested not only through preventive measures to preclude the occurrence of violations, but also through legal protection of a repressive nature when a violation of rights has already occurred (Hadjon, 1987). In the context of personal data processing, repressive legal protection is actualized through the liability imposed upon the Personal Data Controller in the event that data processing is conducted in a manner non-compliant with the provisions of laws and regulations or inflicts injury or loss upon the Personal Data Subject. Therefore, the status of a fintech lending provider as a Personal Data Controller gives rise not only to the authority to process personal data, but also to a legal obligation to account for and bear liability for every personal data processing activity carried out in the course of operating its services.

Law Number 27 of 2022 concerning Personal Data Protection imposes a multitude of obligations upon the Personal Data Controller in executing personal data processing operations. These obligations encompass, *inter alia*, conducting the processing of personal data in a limited, specific, lawful, and transparent manner, ensuring the security of the processed personal data, maintaining the confidentiality of personal data, and fulfilling the rights of Personal Data Subjects as prescribed under the Personal Data Protection Law (Jonathan Matthew, 2024). Furthermore, the Personal Data Controller is also required to implement the principle of accountability, namely being capable of accounting for the entirety of the personal data processing operations conducted. Consequently, the liability of a Personal Data Controller does not terminate upon the acquisition of personal data, but remains attached and continuous throughout the processes of collection, storage, use, disclosure, up to the erasure of said personal data.

When construed in relation to the aforementioned provisions, Article 3.11 of the Terms of Service of the Kredit Pintar Platform stipulates that the user warrants that they have obtained consent from the party registered as an emergency contact, and shall release, hold harmless, and indemnify the provider against any losses, claims, or legal lawsuits arising in connection with communications made to the said emergency contact. This clause fundamentally constitutes a mechanism for transferring legal risk to the user regarding the use of the emergency contact's personal data. Nevertheless, the status of the provider as a Personal Data Controller remains inherently attached pursuant to Law Number 27 of 2022 concerning Personal Data Protection; hence, the obligation to execute personal data processing lawfully, securely, and accountably cannot be abated or waived solely based on a unilateral declaration within a contractual clause (Zhou, Zhang, Han, Zhu, & Wang, 2023). Therefore, the existence of such a clause necessitates a rigorous analysis to assess whether the transfer of liability to the user aligns with the principle of Personal Data Controller liability under the Personal Data Protection Law.

Examined under the provisions of Law Number 8 of 1999 concerning Consumer Protection, a clause requiring the user to release and indemnify the provider from and against any claims or legal lawsuits arising from communications with the emergency contact may potentially be qualified as an exculpatory clause that shifts the liability of the business actor (Dr. H. Sukawi Sutarip, 2024). Yet, Article 18 paragraph (1) letter a of the Consumer Protection Law expressly prohibits business actors from inserting standard clauses that declare a transfer of liability to consumers. On the other hand, pursuant to Law Number 27 of 2022 concerning Personal Data Protection, the provider's position as a Personal Data Controller remains indissoluble, so that the obligation to protect personal data and account for its processing cannot be derogated from by means of a standard clause in an agreement (Fajar Nugroho Handayani, 2020). Consequently, the compatibility of the clause with the principle of Personal Data Controller liability as well as consumer protection principles, which demand an equitable balance of the rights and obligations of the parties, is highly questionable.

Based on the foregoing description, platform liability as a Personal Data Controller is an inherent legal consequence of any personal data processing activities conducted within the operation of fintech lending services. From the perspective of repressive legal protection, a provider cannot absolve itself of or transfer its liability to the user merely through standard clauses that compel the user to provide warranties or indemnities against claims arising from the processing of emergency contact personal

data. Should the processing of personal data be executed in non-fulfillment of the provisions of Law Number 27 of 2022 concerning Personal Data Protection and inflict injury or loss upon the Personal Data Subject, the provider remains subject to liability in accordance with the applicable legal mechanisms. Therefore, the contractual arrangements governing the processing of emergency contact personal data in fintech lending agreements must reflect the principle of accountability, the protection of the rights of the Personal Data Subject, and an equitable balance of the rights and obligations of the parties, in order to establish legal certainty and effective legal protection.

4. CONCLUSION

First, the processing of emergency contact personal data in fintech lending agreements can, in principle, be declared valid provided that it satisfies the lawful basis for processing regulated under Article 20 of Law Number 27 of 2022 concerning Personal Data Protection. Such validity is not determined solely by the inclusion of a contractual clause stating that the user has obtained consent from the emergency contact, but also depends heavily upon the fulfillment of the core principles of personal data protection, such as legality, transparency, accountability, as well as respect for the rights of the Personal Data Subject. Therefore, a fintech lending provider, in its capacity as a Personal Data Controller, remains under an obligation to ensure that the processing of an emergency contact's personal data is predicated upon a valid legal basis and executed through mechanisms that guarantee legal protection for the data owner. Accordingly, clauses that merely ground personal data processing on the unilateral declaration of the user are insufficient to guarantee the validity of personal data processing under Law Number 27 of 2022 concerning Personal Data Protection.

Second, a fintech lending platform, as a Personal Data Controller, bears an inherent legal liability for every instance of emergency contact personal data processing carried out in the course of operating its services. This liability encompasses the obligation to execute data processing in a lawful, transparent, and accountable manner, as well as to guarantee the protection of the rights of the Personal Data Subject as prescribed under Law Number 27 of 2022 concerning Personal Data Protection. Consequently, clauses within an agreement that obligate the user to release or indemnify the provider from and against claims arising from the processing of emergency contact personal data do not extinguish the legal liability of the provider as a Personal Data Controller. Should the processing of personal data be conducted in contravention of the provisions of laws and regulations and inflict loss or injury upon the Personal Data Subject, the provider may nonetheless be held liable in accordance with the applicable legal mechanisms. As a result, the contractual provisions governing the processing of emergency contact personal data in fintech lending agreements must mirror the principles of accountability, consumer protection, and personal data protection in order to achieve legal certainty and provide effective legal protection for all concerned parties.

REFERENCES

Aprillia Mieke U. (2025). *Membongkar Masalah Gagal Bayar Pinjaman online, Tinjauan Praktis Hukum Perdata*. Banjarnegara: PT Penerbit Qriset Indonesia.

Dadan Kurniawan. (2026). *Cara Gagal Bayar Hutang Pinjol: Panduan Praktis Mengahdapi Gagal Bayar, Perlindungan Data Pribadi dan Strategi Pemulihan Nama Baik Sesuai Aturan OJK*. Karawang: Afdan Rojabi Publisher.

Daffa Arya Prayoga, Jadmiko Anom Husodo, & Andiana Elok Puri Maharani. (2023). Perlindungan Hukum Terhadap Hak Warga Negara Dengan Berlakunya Undang-Undang Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional. *Jurnal Demokrasi Dan Ketahanan Nasional*, *2*(2), 191.

Doni Harianto, Adithia Permana Sinaga, & Fajriansyah. (2025). Analisis Yuridis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Kontak Darurat Sepihak di Platform Pinjaman Online Legal (Studi Kasus Platform Ada Modal). *Jurnal Hukum Ius Publicum*, *6*(1), 222.

Dr. H. Sukawi Sutarip. (2024). *Rekonstruksi Pengaturan Eksekusi Hak Tanggungan di Indonesia Berlandaskan Asas Keadilan*. Semarang: CV Lawwana.

Fajar Nugroho Handayani. (2020). *Penggunaan Klausula Baku Yang Dilarang Menurut Hukum Perlindungan Konsumen*. Ponorogo: Uwais Inspirasi Indonesia.

Gita Theresa. (2024). Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech P2P Lending di Indonesia. *Jurnal Darma Agung*, *32*(3), 357.

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.

Jebaru, R. A., & Widiatno, M. W. (2026). Perlindungan Hukum Bagi Prosesor Data Pribadi Dalam Melaksanakan Pemrosesan Data Pribadi Menggunakan Aplikasi Sistem Informasi Kependudukan. *Pengabdian Masyarakat Dan Riset Pendidikan*, *4*(3), 19570.

Jonathan Matthew. (2024). Kesadaran Urgensi Peran Pengendali dan Prosesor data Pribadi dalam Rangka Perlindngan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Hukum Tora*, *10*(1), 126.

Kinanti, W., Ramadhani, S., & Wiraguna, S. A. (2025). Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan. *Journal Perspektif Administrasi Publik Dan Hukum*, *2*(2), 158–175.

Kredit Pintar. (2026). *Terms of Service*.

Marzuki, P. M. (2021). *Penelitian Hukum (Edisi Revisi)*. Jakarta: Kencana.

Muhammad Faiq Nizam. (2026). *Urgensi Perlindungan Data Pribadi Lewat Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*.

Natasya Klarisa Paruntu, & Amad Sudiro. (2025). Pergeseran Paradigma Pemulihan Aset Dalam Tindak Pidana Korupsi Untuk Mewujudkan Optimalisasi Pengembalian Kerugian Negara. *Jurnal USM Law Review*, *8*(3), 1903–1929. https://doi.org/10.26623/julr.v8i3.12888

Otniel Yustisia Kristian. (2022). Perlindungan Hukum Pengguna Layanan Fintech p2p Lending dari Tindak Pidana Ekonomi dan Terhadap Penyedia Layanan Fintech P2P Lending Ilegal. *Majalah Hukum Nasional*, *52*(2), 298.

Pranoto. (2025). Perlindungan Hukum Terhadap Emergency Contact Dalam Pinjaman Online Peer to Peer Lending. *Jurnal Universitas Sebelas Maret*, *13*(2), 241.

Republik Indonesia. (2022). *Pasal 20 ayat 1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Tegar Uji Asetko Runto, Tahasak Sahay, & Andika Wijaya. (2026). Perlindungan Hukum Terhadap Emergency Contact Dalam Pinjaman Online Peer to Peer Lending. *Jurnal Universitas Sebelas Maret*, *4*(2), 2851.

Zhou, W., Zhang, D., Han, G., Zhu, W., & Wang, X. (2023). A blockchain-based privacy-preserving and fair data transaction model in IoT. *Applied Sciences*, *13*(22), 12389.