GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v4i2

The Urgency of Recognizing the 'Opt-Out Right' to Protect Consumer Personal Data in P2P Lending Fintech

Nadia Carolina Weley[1*], Shenti Agustini[2], David Tan[3], Tony Wibowo[4], Tony Tan[5]
[1]Universitas Internasional Batam, Batam, Indonesia, nadia.carolina@uib.ac.id
[2]Universitas Internasional Batam, Batam, Indonesia, shenti.agustini@uib.ac.id
[3]Universitas Internasional Batam, Batam, Indonesia, david.tan@uib.ac.id
[4]Universitas Internasional Batam, Batam, Indonesia, tony.wibowo@uib.ac.id
[5]Universitas Internasional Batam, Batam, Indonesia, tony@uib.ac.id

*Corresponding Author: nadia.carolina@uib.ac.id[1]

Abstract: Financial Technology (FinTech) has significantly advanced financial services in the digital era, with Peer-to-Peer (P2P) lending platforms emerging as a major example. While these platforms provide financial assistance, many operate under the principle of "forced consent," where users are required to agree to unnecessary data processing, such as for marketing or data analysis, as a condition for accessing core services. This practice violates the "lawful consent" principle outlined in the 1945 Constitution of the Republic of Indonesia and is implicitly prohibited under Law Number 27 of 2022 on Personal Data Protection and regulations by the Financial Services Authority. This study proposes a concrete solution by advocating for the adoption of the "Right to Opt-Out," a principle effectively implemented by the European Union through the General Data Protection Regulation (GDPR). The Right to Opt-Out allows individuals to refuse or limit the use of their personal data without losing access to essential services. Using a normative legal research method with a statutory approach, the study recommends incorporating the Right to Opt-Out into Indonesia's data protection framework, enhancing legal certainty and empowering consumers to control their personal data in P2P lending services.

Keywords: Forced Consent, Fintech, Peer-to-Peer Lending, Personal Data Protection.

INTRODUCTION

Indonesia, with its large digital population, stands as one of the key markets for the growth of financial technology (fintech), which not only serves digital payment services but also online lending or Peer-to-Peer (P2P) Lending fintech (Jange et al., 2024). The widespread digital transformation in Indonesia is driven by the adoption of technology and increasing internet accessibility, creating significant opportunities for inclusive economic growth by involving all segments of society in the financial sector (Jange et al., 2024). According to the World Bank (2023), Indonesia's population reaches 277.5 million, with over 220 million active internet users, representing more than 70% of the country's

population, based on data from the Indonesian Internet Service Providers Association (APJII, 2024; Komdigi, 2024). However, despite the rapid and successful growth of fintech in Indonesia, it also brings challenges for consumers using these services. Research conducted by (Syahruddin & Zulfa, 2024) highlights one of the legal issues consumers face: the application of the forced consent principle, where individuals are coerced into giving consent for the use of their personal data because they have no alternative to access certain services provided by service providers. The issue of forced consent affects 76.1% of users of P2P lending fintech in Indonesia, who provide personal data to access services like SMS, Calendar, Photos, media, and files on their devices, phone calls, taking pictures and recording videos, location or GPS data, and Audio Contacts. RupiahPlus, a leading P2P lending fintech application, has been flagged for forcing consent from its users, resulting in contacting individuals from a user's contact list even though they were not the designated emergency contacts. The Indonesian Financial Technology Association (Aftech), a platform for fintech companies and institutions, has indicated that RupiahPlus violated two key regulations: FSA Regulation No. 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (FSS Consumer Protection) and Ministerial Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems (MCDA Regulation on Electronic Personal Data Protection) (Syahruddin & Zulfa, 2024). In Indonesia, regulations concerning forced consent have not been explicitly addressed in the Personal Data Protection Law No. 27 of 2022. While this law sets general principles for personal data protection, including consent as the basis for data processing, it does not specifically define conditions or limitations that can be categorized as forced consent (Komdigi, 2024). This ambiguity creates a regulatory gap, a legal void that leads to uncertainty in the enforcement of personal data protection, particularly when individuals feel "forced" to give consent in order to access specific digital services or products (Khan, 2021).

The practice of forced consent in P2P lending fintech applications in Indonesia presents a critical legal issue regarding the validity of consent (Komdigi, 2024). P2P lending fintech applications in Indonesia, whether registered or not with the Financial Services Authority (FSA), often force users to give consent for access to personal data, such as contacts, location, and photo galleries, as a mandatory requirement to use the service (Asimah, 2021). This raises the question of whether consent in such cases can be considered valid under the law, especially when data processing is not directly related to the core services being provided (Kusuma & Roisah, 2022). This practice conflicts with the principle of personal data protection, which mandates that consent must be freely given, specific, informed, and unambiguous, as outlined in Indonesia's Personal Data Protection Law (Article 21, paragraph (1)(c)). Moreover, it infringes upon the fundamental right to privacy guaranteed by Article 28G of the 1945 Constitution of the Republic of Indonesia, which provides every individual with the right to control their personal data. However, enforcement remains weak, as highlighted by (Manggala et al., 2024), and the lack of strong oversight continues to expose users to data misuse. While the FSA has attempted to address illegal P2P lending applications, the number of data violations indicates that the monitoring and law enforcement mechanisms are still far from ideal (Ju et al., 2021).

Research by (Setiawan et al., 2024) explores various aspects of data security in the digital context. This study shows that the existing regulations in Indonesia are not fully protective of user data from misuse. The main weakness is the lack of stringent enforcement against privacy violations, as well as users' low awareness of the risks of data leakage. Syifa and (Adam, 2024) analyze the protection of personal data in technology-based lending and highlight the gaps in the legal protection mechanisms, which make borrowers vulnerable to data misuse. However, the research lacks exploration of the role digital platforms play in mitigating these risks. The study by (Noer et al., 2024) discusses the regulatory impact on

fintech services such as Spaylater, including aspects of consumer protection law. While fintech regulations are fairly comprehensive, there are legal gaps affecting fintech operations, such as limited government oversight mechanisms. However, this research does not address personal data protection in platforms like Shopee. (Jange et al., 2024), in their research on the transformation of financial services through fintech, explain the changes in financial services due to technological adoption aimed at improving financial inclusion and highlight the legal protection deficiencies and privacy risks. The limitation of this research is its lack of specific focus on personal data protection in the fintech sector. Lastly, (Najwan & Sudarwanto, 2024) examine legal protection against the misuse of personal data by illegal online lending services, revealing the weak oversight of illegal actors and the minimal sanctions imposed. The drawback of this study is its failure to cover technological solutions that could be used to reduce risks related to personal data misuse.

This body of research highlights significant gaps in legal protections, enforcement, and regulatory clarity, particularly concerning forced consent and the protection of personal data in Indonesia's fintech sector (Weley & Disemadi, 2022). The central legal issue addressed in this study is whether consent can be considered valid when consumers are forced to accept unnecessary data processing as a condition for accessing essential services on P2P lending platforms. This research differentiates itself from previous studies by focusing on the urgency of recognizing individuals' right to refuse or withdraw consent regarding the collection, use, or sale of their personal data, especially in the context of forced consent. The study provides a theoretical foundation for understanding the balance between technological innovation and the protection of individual privacy rights and argues that such forced consent cannot be considered valid under the principles of lawful consent outlined in data protection law. Furthermore, this research offers a concrete legal recommendation for the government to formulate more effective data protection regulations that ensure consumers' rights are upheld without stifling innovation in the fintech sector. It also provides valuable insights for fintech industry players to design more fair, transparent, and user-centric data collection and processing policies, which will foster greater consumer trust in their services. The relevance of this study becomes even more significant as the rapid development of peer-to-peer lending technologies outpaces consumer understanding of how their personal data is being used.

METHOD

This research employs a normative legal research method, focusing on analyzing forced consent in personal data protection within Indonesia's fintech sector (Jange et al., 2024). The study uses a statutory approach to examine the legal instruments directly related to the issue. The approach utilized is the statutory approach, which allows the researcher to examine and analyze the existing legal instruments to understand the legality and implications of forced consent practices (Tan, 2021). The primary legal materials include regulations such as Law No. 27 of 2022 on Personal Data Protection, the 1945 Constitution of the Republic of Indonesia, GDPR, Ministerial Regulation No. 20 of 2016, FSA Regulations No. 22/2023 and No. 77/POJK.01/2016, and other relevant laws such as Law No. 19 of 2016 and CCPA. These materials are the foundation of the study, directly addressing the legal issue. Secondary legal materials comprise commentaries, scholarly articles, and analyses that help interpret these laws. Tertiary legal materials include resources like legal dictionaries or digests offering brief summaries or interpretations. Data collection was conducted through document studies, examining these primary, secondary, and tertiary legal materials (Disemadi, 2022).

RESULTS AND DISCUSSION

The Legal Construction of Forced Consent in Protecting Consumer Personal Data in P2P Lending Fintech within the Framework of Indonesian Law

Personal data protection has become an integral issue in the era where information technology serves as the primary means of digital communication. Personal data protection is not only used to safeguard the confidentiality of personal information but also several dimensions that have substantial relevance for both individuals and society. In Indonesia, personal data protection is particularly important in the use of P2P lending fintech applications, as personal data is often a requirement to access the core features provided by service providers (Neta et al., 2022). However, the collection and use of personal data raises concerns for consumers, as it holds strategic value for both users and third parties who may exploit the data for commercial or other purposes without consumer consent. Non-compliance with the personal data protection principles by service providers can open opportunities for exploitation, which harms consumers (Gladys et al., 2024). This can occur in several forms, such as misuse of information, digital fraud, and privacy violations. In practice, many fintech service providers adopt the forced consent approach, where consumers wishing to use the features provided by the service provider are coerced into agreeing to data processing without alternative options to access the main service. This forced consent approach not only violates consumers' fundamental privacy rights but also represents a significant issue requiring serious intervention and stricter data protection measures (Sholehuddin et al., 2024).

Forced consent refers to situations where an individual provides consent not voluntarily, but due to pressure, coercion, or an unavoidable obligation to access a particular service offered by the service provider (Sholehuddin et al., 2024). Under the personal data protection regulations in Indonesia, forced consent contradicts the applicable laws and the basic principle of freely given consent, which requires that consent be given voluntarily, without any coercion or threat of negative consequences (Lestari & Mujib, 2022). In the P2P lending fintech industry, forced consent occurs when consumers are required to grant access to their personal data, such as contacts, location, gallery, voice, and other data, as a mandatory condition to proceed with a financial transaction. In this situation, consumers have no alternative but to accept the terms presented, as refusal would result in losing access to the essential services needed. The regulation concerning this is outlined in the GDPR, the privacy and security law enacted by the European Union on May 25, 2018, which applies to all organizations within the EU (Amer et al., 2024). The issue of forced consent in the GDPR is addressed in Article 7, Article 21, and Recital 43, Paragraph 2, regarding freely given consent, which states, "Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

The right to privacy and personal data protection in Indonesia is an integral part of human rights, guaranteed by the Indonesian Constitution, specifically Article 28G, Paragraph (1) of the 1945 Constitution of the Republic of Indonesia (The 1945 Constitution), which states, "Every person shall have the right to personal, family, honor, dignity, and property protection, as well as the right to feel secure and protected from threats or fear of doing or not doing something that is a basic human right.". (Pradana & Saragih, 2024) Article 28G of the The 1945 Constitution serves as the foundation for every individual's right to feel secure and protected from privacy violations, including the protection of personal data. Therefore, the management of personal data in Indonesia must be conducted with respect for the individual's autonomous rights, particularly in the era of industrial revolution (Fauzie, 2024). In this context, based on national constitutional law, the forced consent principle used by P2P lending fintech service providers, where individuals are forced to consent to the use of their personal data without alternatives, violates the principle of freedom and individual control

over the use of their personal information. Furthermore, the 1945 Constitution also guarantees legal certainty and fairness in the management of personal data, aiming to prevent the exploitation of data that harms individuals, as outlined in Article 28D, Paragraph (1), which reads, "Every person shall have the right to recognition, guarantees, protection, and fair legal certainty, as well as equal treatment before the law."

The regulation of personal data protection in Indonesia is specifically governed by the Personal Data Protection Law, which ensures security and privacy in the digital era. The law emphasizes the principles of transparency, fairness, and voluntary consent as the foundation for managing personal data in Indonesia. Essentially, the Personal Data Protection Law protects individuals from potential misuse and dissemination of personal data, one of which is reflected in Article 20, Paragraph (2), letter a, which states, "(2) The basis for personal data processing as referred to in paragraph (1) includes: a. explicit and valid consent from the Data Subject for one or more specific purposes communicated by the Data Controller to the Data Subject." This highlights the importance of explicit consent in the collection and management of personal data and asserts that every individual has full control over their personal data. The reinforcement of regulations concerning Article 20, Paragraph (2) is further strengthened by Article 15, Paragraph (1) of the Personal Data Protection Law, which stipulates that personal data processing must be aligned with specific purposes that must be agreed upon by the data owner. Additionally, the Personal Data Protection Law also provides an administrative sanction mechanism, as outlined in Article 57, Paragraph (2), which reads, "(2) The administrative sanctions referred to in paragraph (1) include: a. written warning; b. temporary cessation of personal data processing activities; c. deletion or destruction of personal data; and/or d. administrative fines." Articles 36 and 38 of the Personal Data Protection Law support service providers in ensuring the protection of users' data (Murdayantin et al., 2023).

In addition to the Personal Data Protection Law, privacy regulations in the digital era, particularly concerning P2P lending fintech, are also governed by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law), the Ministerial Regulation on Electronic Personal Data Protection (MCDA), Financial Services Authority Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending Services (FSS fintech), and FSS Consumer Protection. The ITE Law regulates the protection of personal data through Article 26, Paragraph (1), which states, "Unless otherwise stipulated by law, the use of any information through electronic media concerning an individual's personal data must be done with the consent of the person concerned." This emphasizes that personal data use requires the consent of the data owner, reinforcing the fundamental principle of lawfulness in data processing. Meanwhile, the FSS fintech regulation addresses forced consent, although not explicitly, through Article 26, letter b, which states, "b. ensuring the availability of authentication, verification, and validation processes that support non-repudiation in accessing, processing, and executing personal data, transaction data, and financial data managed." This article emphasizes that the execution of personal data must be preceded by consent from the data owner. Additionally, Article 29 of the FSS fintech regulation mandates that service platforms must have adequate data protection systems to ensure the confidentiality and security of consumer information, preventing users from potential personal data breaches. Furthermore, the FSS Consumer Protection regulation addresses the prohibition of forced consent in P2P lending fintech applications through Article 4, Paragraph (1), which reads, "Financial Service Providers (PUJK) must act in good faith when conducting business activities and/or providing products and/or services to prospective and/or existing consumers." The principle of forced consent is inconsistent with the good faith requirement outlined in this regulation. If service providers violate this provision, they will be subject to administrative sanctions as outlined in Article 4, Paragraph (5) and Paragraph (6) (Halbert et al., 2023).

The regulations enacted in Indonesia have established a technical foundation for data protection within the digital ecosystem and personal data protection. However, the implementation of these regulations faces challenges that are inconsistent with real-world practices in Indonesia (Pratama & Multazam, 2024). The legal certainty theory proposed by M. Yahya Harahap emphasizes the importance of clear, consistent, and enforceable regulations to create justice and protection for the public. Regarding forced consent, although existing regulations in Indonesia, such as the 1945 Constitution, Personal Data Protection Law, Ministerial Regulation on Electronic Personal Data Protection, FSS fintech, and FSS Consumer Protection, do not explicitly address forced consent, they are sufficient to cover personal data protection. However, they do not guarantee legal certainty for consumers in cases of forced consent. Substantively, the Personal Data Protection Law and FSS provide a clear legal basis, but forced consent still occurs, where consumers are coerced into agreeing to unfair terms and conditions as a prerequisite for using P2P lending fintech services (Harista et al., 2021). This imbalance creates an uncomfortable position for users, as service providers fail to fully meet the good faith and voluntary principles. From a procedural perspective, service providers that enforce forced consent are also unable to adequately protect the personal data provided by users, leading to data breaches that are either unreported or not effectively addressed (Harista et al., 2021).

The implementation of such practices undermines public trust in digital media usage, despite the legal framework already established in Indonesia. The lack of detailed technical guidance to ensure that user consent is voluntary creates a regulatory gap and results in ambiguous standards, which can be exploited by service providers to evade legal responsibility (Harista et al., 2021). The FSA, as a key regulatory body, plays a central role in maintaining the integrity and stability of Indonesia's financial sector, including regulating the fintech ecosystem. The FSA is responsible for ensuring that P2P lending fintech applications comply with consumer data protection principles to support the rapid development of technology, which increases the risks of privacy violations and data misuse. One step the FSA can take is to conduct comprehensive oversight of P2P lending providers and issue regulations that can govern the financial sector in the era of industrial revolution, including the collection, storage, and use of consumers' personal data. Additionally, the FSA can implement oversight through the use of Regulatory Technology (RegTech), allowing for early detection of violations. As the main regulator, the FSA also imposes strict sanctions on providers who violate the rules, such as revoking operating licenses or imposing administrative fines directly on P2P lending fintech service providers. The administrative sanctions imposed by the FSA aim to deter non-compliance and encourage P2P lending providers to prioritize compliance.

Forced consent in P2P lending services poses a serious threat to consumer privacy in Indonesia. To address this issue, an approach that includes both regulations and strict oversight is required. The regulations currently in place in Indonesia need to be accompanied by clear technical guidelines that define the boundaries of consumer data usage and explicitly prohibit the forced consent principle, which can harm service users. Adjustments to the legal framework in Indonesia should align with international standards, such as the General Data Protection Regulation (GDPR), to ensure more comprehensive protection. In this context, the FSA and MCDA need to collaborate and implement regular audit systems along with accessible complaint mechanisms, which could help detect and prevent unethical practices in Indonesia, especially in the use of P2P lending fintech applications (Syahputra & Fibrianti, 2024).

Proposed Recognition of the "Opt-Out Right" as a Legal Solution to Forced Consent in Protecting Consumer Personal Data

The opt-out right is an important component in the framework for personal data protection in Indonesia, granting consumers the ability to reject the processing of certain data without affecting their access to essential services or features, especially in P2P lending fintech applications. This concept of the opt-out right offers a solution to the criticisms of forced consent, where consumers are compelled to agree to data processing as a condition for using services, without any viable alternatives. The opt-out right also empowers consumers to have control over their personal data, balancing the interests of users with business needs (Syaiful & Sugiyono, 2024). GDPR, which serves as a global benchmark for personal data protection, includes the implementation of the opt-out right to define limits on the use of personal data for purposes such as marketing, tracking, or third-party sales. The opt-out right further strengthens consumer awareness of the value of their personal data and encourages companies to take greater responsibility for managing it. However, the practical application of the opt-out right also depends on public response and effective implementation (Kusumaningsih & Yulianingsih, 2023). Consumers must be informed of their rights, and some companies may complicate the opt-out process with cumbersome procedures. In Indonesia, the recognition of the opt-out right would be a progressive step toward protecting individual privacy in the digital age. By allowing consumers to reject data processing without facing negative consequences, the opt-out right not only protects privacy but also fosters stronger trust between users and service providers (Disemadi, 2021).

As a global regulation governing personal data protection, the GDPR includes provisions regarding the opt-out right as a solution to forced consent practices that violate good faith. The GDPR's Recital 43 addresses the issue of freely given consent, emphasizing the importance of voluntary consent in data processing. Specifically, Article 21 of the GDPR outlines the opt-out right, stating: Article 21, Paragraph (1): 'The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims." Article 21, Paragraph (2): "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing." Article 21, Paragraph (3): "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes." These provisions establish that data subjects, in this case, service users, have the right to object to the processing of their data for reasons related to their specific situation, at any time. If personal data is being processed for direct marketing purposes, users can opt-out and prevent their data from being used for such purposes, thus halting the processing that does not align with their consent. By incorporating similar mechanisms in Indonesia's regulatory framework, particularly for P2P lending fintech services, the country can better safeguard consumer privacy, align with international standards, and promote responsible data handling by service providers (Halizah & Mardikaningsih, 2024).

Furthermore, Article 7 of the GDPR also stipulates that data processing must be based on consent, where the data controller or service provider must be able to demonstrate that the data subject has consented to the processing of their personal data without coercion. Additionally, the data subject has the right to withdraw their consent at any time, provided that this does not affect the legality of processing based on the consent before its withdrawal. The text of the article reads: "(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal

data. (2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. (3) (1) The data subject shall have the right to withdraw his or her consent at any time. (2) The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. (3) Prior to giving consent, the data subject shall be informed thereof. (4) It shall be as easy to withdraw as to give consent." In addition to the GDPR, other international regulations governing the opt-out right include the CCPA and California Privacy Rights Act (CPRA), which regulate consumer privacy protection in the United States (Hunter et al., 2024).

The CCPA is a regulation enacted to protect privacy data and consumer rights in the U.S. These two laws provide consumers with the right to refuse the sale of their personal data and strengthen transparency and accountability for service providers, particularly in P2P lending fintech. The opt-out right mechanism is regulated through Article 1798.120, Consumers' Right to Opt-Out of Sale or Sharing of Personal Information, which states: "(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing. (b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the 'right to opt-out' of the sale or sharing of their personal information." This article affirms that consumers also have the right to limit the use of sensitive data, such as geographic location, sexual orientation, and health status. With this strengthened protection, CPRA not only continues the transparency principles of CCPA but also enhances consumers' ability to protect highly personal data (Halizah & Mardikaningsih, 2024). The obligation for service providers to offer an opt-out option aims to create a balance between business needs for utilizing data and individuals' privacy rights, with service providers required to ensure that this option is easy to access and not confusing, as outlined in the implementation guidelines of this law. Furthermore, the CPRA establishes the California Privacy Protection Agency (CPPA), an independent regulatory body tasked with ensuring compliance with these privacy regulations, including overseeing the opt-out mechanism. Any violations in limiting the deletion of personal data or in failing to protect personal data will result in penalties imposed by the CPPA (Marikyan, 2023).

Regulation on personal data protection in Indonesia, particularly the Personal Data Protection Law (PDP Law), still leaves several legal gaps regarding consumer privacy and security. One significant gap is the absence of a clear regulation on the opt-out right, which gives consumers the ability to reject the collection, use, and distribution of their personal data by third parties. This is particularly concerning given the rapid growth of fintech, which relies heavily on the collection of personal data as the foundation for its operations (Marikyan et al., 2023). Fintech services, particularly P2P lending applications, use and leverage consumer data for analysis, marketing, and risk profiling, without offering consumers the opportunity to limit or refuse the use of their personal data. This lack of control results in consumers not having full authority over their personal data, making them vulnerable to misuse, data manipulation, privacy violations, or the sale of their data to irresponsible parties. In comparison, developed countries such as the European Union have adopted more progressive data protection policies through the GDPR, which explicitly outlines the opt-out right as part of consumer rights to protect their privacy and avoid data misuse. This regulation not only provides consumers with a sense of security but also encourages companies to be more

transparent and responsible in managing personal data. The recognition of the opt-out right in Indonesia has become an urgent need in light of the rapid advancement of information and digital technologies, coupled with the increasing threats to individual privacy. In personal data protection, the opt-out right must be explicitly regulated to ensure a legal basis with effective implementation. This regulation would provide greater control to individuals, as data owners and service users, over their personal data. The legal implications of the opt-out right in Indonesia would strengthen the fundamental privacy and data protection principles as outlined in the GDPR in the EU (Xia et al., 2024). In Indonesia, the opt-out right could be incorporated into the Personal Data Protection Law, where the regulation must include clear mechanisms for individuals to object to the use of their personal data and require service providers to respect the requests made by data owners. The recognition of the opt-out right also requires strict oversight by data protection authorities to ensure legal certainty and that the opt-out right is consistently and transparently implemented within society. By integrating the opt-out right into the national legal framework, Indonesia would not only protect its citizens from potential personal data misuse but also foster a responsible and sustainable digital ecosystem. This move would position Indonesia as a progressive country in data protection in the digital age, particularly in the fintech sector and P2P lending fintech applications.

The progressive legal theory introduced by Satjipto Rahardjo serves as a foundation for responding to the dynamic needs of modern society. This theory emphasizes that law is not a static entity but a living instrument that functions to meet the interests of society in a flexible and adaptive manner. In the era of the industrial revolution, the relevance of progressive theory is increasingly evident, particularly in the recognition and protection of consumer rights and personal data, where the opt-out right can be a tangible manifestation of applying progressive legal theory in digital transactions (Hansmann & Binder, 2023). This allows consumers to reject the use of their personal data for marketing activities or data collection they do not consent to. The recognition of the opt-out right in Indonesia must also be pursued with a more humanistic legal approach, prioritizing individual protection over corporate interests (Soekarni, 2024). The implementation of the opt-out right in service provision must be designed with principles of justice, accessibility, and transparency, ensuring that service providers have a moral and legal responsibility to ensure that consumers can opt-out of certain services without facing unnecessary technical or procedural barriers (Fatorachim et al., 2025).

However, the opt-out mechanism should be realized through several approaches, including: service providers must offer intuitive and easy-to-use digital interfaces, such as placing the opt-out button or option in strategic locations as part of the application or website. The language used should be simple and direct, free of confusing technical jargon (Hunter et al., 2024). Clear notifications should be provided to users, particularly when they first register, especially if there are changes to policies that include clear information about users' right to opt-out and the potential consequences of their decision without disadvantaging either the consumer or the service provider. The main impact of implementing the opt-out right is the creation of a more transparent and accountable digital ecosystem, where technology companies and digital service providers are required to uphold the principle of openness in explaining how data is used (Padden & Öjehag-Pettersson, 2021). As a result, public trust in the digital ecosystem can be increased, which is a crucial element in supporting digital transformation in Indonesia. On the other hand, the opt-out right can also encourage innovation in data management, where companies will strive to develop more ethical and consumer-friendly technologies to avoid privacy violations. This opens up opportunities for the growth of business models that focus on consumer interests, making the digital ecosystem more inclusive and sustainable.

In addition to regulations regarding the opt-out right, the government plays a crucial role in ensuring that the implementation of this right aligns with the principles of personal data protection and transparency as stipulated by the hierarchy of laws in Indonesia. Government agencies such as the FSA and MCDA bear the primary responsibility for overseeing compliance with existing regulations. This begins with the implementation of regular audits for companies that manage personal data, ensuring that they truly respect consumer choices as service users. The audit process conducted by supervisory institutions should include data security evaluations, privacy incident reporting, and the success rate of the opt-out mechanism. In this regard, regulations must also establish sanctions, such as administrative penalties like business license revocation, fines, and other legal actions that can provide a deterrent effect, ensuring that the opt-out right operates effectively in society. By adopting global best practices, such as the GDPR in the EU, the implementation of the opt-out right can position Indonesia as a key player in data governance focused on consumer interests. This step not only protects consumers but also strengthens Indonesia's position in the global digital economy by creating a secure, transparent, and competitive ecosystem (Purnamasari et al., 2025)

CONCLUSION

Forced consent is a prevalent practice in Indonesia's P2P lending fintech sector, where consumers are often required to consent to the collection and use of personal data as a condition for accessing services. This practice creates a legal imbalance, as it conflicts with the principle of freely given consent, as outlined in Indonesia's Personal Data Protection Law. While the law addresses personal data protection, it does so in a general manner, leaving gaps in ensuring that consent is obtained without coercion. This contrasts with the European Union's GDPR, which explicitly mandates that consent must be freely given and provides individuals the ability to access services without being forced to provide unnecessary personal data.

The legal issue at hand is whether consent obtained through coercive means in P2P lending can be considered valid under Indonesia's current framework. The research findings suggest that forced consent, as it is currently practiced, undermines consumer privacy rights and leaves them vulnerable to misuse of their personal data. To address this, the article proposes the introduction of the "opt-out right" in Indonesia's personal data protection regulations. This legal provision would allow consumers to refuse or limit the use of their personal data for non-essential purposes, such as marketing or data analysis, without losing access to core services. By integrating the opt-out right into the regulatory framework, consumers would gain greater control over their personal data, and P2P lending fintech providers would be incentivized to implement more transparent and responsible data management practices.

REFERENCES

Amer, N., Lubis, A. F., Muhtar, M. H., Saija, V. J. E. ., Putri, V. S., & Setiawan, B. (2024). Implications of The Constitution For Political Neutrality in The Dynamics of Law and Democracy. Journal De Facto, 10(2), 283–302. https://doi.org/10.36277/jurnaldefacto.v10i2.189

Asimah, D. (2020). To overcome the constraints of proof in the application of electronic evidence. *Jurnal Hukum Peratun*, *3*(2), 97-110. https://doi.org/10.25216/peratun.322020.97-110.

Disemadi, H. S., & Regent, R. (2021). Urgensi Suatu Regulasi yang Komprehensif Tentang Fintech Berbasis Pinjaman Online Sebagai Upaya Perlindungan Konsumen di

Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *7*(2), 605-618. https://ejournal.undiksha.ac.id/index.php/jkh/article/view/37991/18850.

Disemadi, H. S. (2022). Lenses of legal research: A descriptive essay on legal research methodologies. *Journal of Judicial Review*, *24*(2), 289-304.

Fatorachian, H., O'Higgins, B., Maldonado, A., Lyons, C., Willis, H., Abbott, L., & Brooks, M. (2025). Navigating the challenges of FinTech startups in the B2C market. Cogent Business & Management, 12(1). https://doi.org/10.1080/23311975.2024.2446696

Halbert, G., Rusdiana, S., & Hutauruk, R. H. (2023). Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(3), 304-321. DOI: https://doi.org/10.55809/tora.v9i3.275

Halizah, S. N., & Mardikaningsih, R. (2024). Legal Perspective on Consumer Personal Data Protection in Fintech Services. *Sapientia et Virtus*, *9*(2), 476-489. https://doi.org/10.37477/sev.v9i2.533

Hansmann, R., & Binder, C. R. (2023). Promoting synergies for sustainability through peer-to-peer sharing: an analysis of drivers and barriers. *International Journal of Sustainable Development & World Ecology*, *30*(7), 792–813. https://doi.org/10.1080/13504509.2023.2205831

Hasibuan, S. H. M., Nasution, B., Sunarmi, S., & Siregar, M. (2021). Perlindungan Terhadap Nasabah Dalam Pengamanan Financial Technology Peer To Peer Lending. *Iuris Studia: Jurnal Kajian Hukum*, *2*(3), 372-377. DOI: https://doi.org/10.55357/is.v2i3.150

Hunter, S., Chai, A., Morgan, P., Chan, H. F., Torgler, B., & Rohde, N. (2025). Mobile banking apps and the informal economy: evidence from survey data in Indonesia and Bangladesh. *Applied Economics*, *57*(48), 7873–7888. https://doi.org/10.1080/00036846.2024.2393900

Jange, B., Pendi, I., & Susilowati, E. M. (2024). Peran teknologi finansial (fintech) dalam transformasi layanan keuangan di Indonesia. *Indonesian Research Journal on Education*, *4*(3), 1199-1205. https://doi.org/10.31004/irje.v4i3.1007

Ju, A. B., Tng, A., Weley, N. C., Disemadi, H. S. 2021. Perlindungan Nasabah Dalam Penerapan *Electronic Banking* Sebagai Bagian Aktifitas Bisnis Perbankan di Indonesia. Jurnal Perspektif Administrasi dan Bisnis, 2(1). DOI: https://doi.org/10.38062/jpab.v2i1.16

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer networking and applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R. ., Susilowati, I., Sopian, & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. Lex Publica, 11(2), 221–247. https://doi.org/10.58829/lp.11.2.2024.255

Kusuma, P. H., & Roisah, K. (2022). Perlindungan Ekspresi Budaya Tradisional Dan Indikasi Geografis: Suatu Kekayaan Intelektual Dengan Kepemilikan Komunal. *Jurnal Pembangunan Hukum Indonesia*, *4*(1), 107-120. https://doi.org/10.14710/jphi.v4i1.107-120

Kusumaningsih, R., & Yulianingsih, D. (2023). Tantangan regulasi dan perlindungan hukum dalam pinjaman online. *Jurnal Ilmu Sosial dan Humaniora*, *2*(2), 163-178. DOI: https://doi.org/10.57248/jishum.v2i2.311

Komdigi. 2024. Era Baru Perlindungan Data Pribadi. https://www.komdigi.go.id/berita/artikel/detail/era-baru-perlindungan-data-pribadi.

Lestari, Y., & Mujib, M. M. (2022). Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *11*(2), 203-234. DOI: https://doi.org/10.14421/sh.v11i2.2729

Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2024). General data protection regulation: a study on attitude and emotional empowerment. *Behaviour & Information Technology*, *43*(14), 3561–3577. https://doi.org/10.1080/0144929X.2023.2285341

Murdayantin, F. U., Amelia Agustin, & Dita Pebrianti. (2023). Moral dan Etika Notaris di Era Society 5.0: Kajian Fungsi Artificial Intelligence Terhadap Profesi Notaris. *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, *1*(02). Retrieved from https://journal.forikami.com/index.php/dassollen/article/view/396

Neta, Y., Awanisa, A., & Melisa, M. (2022). The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia. *Constitutionale, 3*(1), 19-38. https://doi.org/10.25041/constitutionale.v3i1.2535

Noer, M. R., Damanik, S. R., Sianturi, R., Purba, B., & Batubara, K. A. (2024). Impact of Fintech Regulations on Spaylater Operations As Well As A Review of Spaylater Consumer Protection Laws. *Jurnal Ekonomi dan Bisnis (EK&BI)*, *7*(1), 348-356. https://www.elibrary.ru/ip_restricted.asp?rpage=https%3A%2F%2Fwww%2Eelibrary%2Eru%2Fitem%2Easp%3Fid%3D81934476

Nurcholis, M. R., Suarda, I. G. W., & Prihatmini, S. (2021). Penegakan Hukum Tindak Pidana Pencucian Uang dalam Penyalahgunaan Investasi Aset Kripto. *Jurnal Anti Korupsi*, *11*(2), 21-40. https://journalversa.com/s/index.php/jhkp/article/download/1128/1514/4541

Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies*, *15*(4), 486–503. https://doi.org/10.1080/19460171.2021.1927776

Pradana, M. A. E., & Saragih, H. (2024). Prinsip akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi terhadap GDPR dan akibat hukumnya. *Innovative: Journal Of Social Science Research*, *4*(4), 3412-3425. DOI: https://doi.org/10.31004/innovative.v4i4.13476

Pratama, S. P., & Multazam, M. T. (2024). Kelemahan Kontrak Pintar: Risiko Konsumen dalam Blockchain. *Journal Customary Law*, *1*(3), 11-11. https://journal.pubmedia.id/index.php/jcl/article/view/2870

Purnamasari, H., Azizah, R. N., & Putri, F. A. (2025). Pengaruh Pengaruh Inovasi Teknologi Financial (Fintech) Syariah dan Literasi Keuangan Syariah Terhadap Pertumbuhan Ekonomi. Bertuah Jurnal Syariah dan Ekonomi Islam, 6(1), 213-232. https://ejournal.kampusmelayu.ac.id/index.php/Bertuah/article/view/1125

Sholehuddin, N., Miskam, S., Shahwahid, F. M., Aziz, T. N. R. A., & Mansor, N. (2024). A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN. *Journal of Muwafaqat*, *7*(1), 23-38. DOI: https://doi.org/10.53840/muwafaqat.v7i1.166

Sianturi, C. G. P., Nababan, R., & Siregar, R. J. (2024). Peran Hukum Dalam Melindungi Data Pribadi. *Innovative: Journal Of Social Science Research*, *4*(5), 2607-2624. DOI: https://doi.org/10.31004/innovative.v4i5.15192

Soekarni, M., Adam, L., Thoha, M., Sarana, J., Ermawati, T., Saptia, Y., … Wibowo, M. (2024). Strengthening financial literacy of smallholder farmers through agricultural fintech peer-to-peer lending: evidence and practical implications. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2359011

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. DOI: https://doi.org/10.38035/jlph.v4i4.414

Syaiful, R. D., & Sugiyono, H. (2024). Misuse of Consumer Personal Data Through Illegal Fintech Peer To Peer Lending. *Justisi*, *10*(1), 189-201. DOI: https://doi.org/10.33506/js.v10i1.3003

Syahputra, B. D., & Fibrianti, N. (2024). Independent Authority on Personal Data Protection in Illegal Financial Technology: Capturing Peer-to-Peer (P2P) Lending Issues. *Journal of Private and Commercial Law*, *8*(1). DOI: https://doi.org/10.15294/jpcl.v8i1.3967

Syifa, A. R., & Adam, R. C. (2024). Perlindungan Data Pribadi Nasabah Peminjam dalam Layanan Pinjaman Meminjam Berbasis Teknologi Informasi Berdasarkan Hukum Perlindungan Data Pribadi. *UNES Law Review*, *7*(2), 683-694. DOI: https://doi.org/10.31933/unesrev.v7i2.2352

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

Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463-2478. DOI: https://doi.org/10.31604/jips.v8i8.2021.2463-2478

Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti: Jurnal Hukum*, *4*(2), 79-93. https://doi.org/10.37729/amnesti.v4i2.2151

Xia L, Cao Z, Zhao Y. 2024. Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows. *Risk Manag Healthc Policy*. https://doi.org/10.2147/RMHP.S450082