

Reconstructing Personal Data Protection Institutions for PayLater Users under Law No. 27 of 2022

Irma Dewi Kania^{1*}, Sentosa Sembiring², Catharina Dewi Wulansari³

¹E-mail: dkania87@gmail.com

²E-mail: sentosa@unpar.ac.id

³E-mail: dewi@unpar.ac.id

^{1,2,3}Universitas Katolik Parahyangan, Indonesia

*corresponding author

Article history:

Received in revised form: 08 July 2026

Acceptance date: 26 July 2026

Available online: 15 August 2026

Keywords:

Personal Data Protection; Personal Data Protection Authority; PayLater.

How to Cite:

Kania, I. D., Sembiring, S., & Wulansari, C. D. (2026). Reconstructing Personal Data Protection Institutions for PayLater Users under Law No. 27 of 2022. *Al-Risalah Jurnal Ilmu Syariah Dan Hukum*, 26(2).

<https://doi.org/10.24252/al-risalah.v26i2.71051>

License:

Copyright (c) The authors (2026)



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Abstract

The development of fintech in Indonesia, particularly through PayLater services, has provided the public with easier access to financing while also driving the growth of digital financial inclusion. On the other hand, the use of these services increases risks to the protection of consumers' personal data, such as the misuse of data for debt collection purposes, the disclosure of information to third parties without consent, and data breaches that result in both material and immaterial losses. This issue is further complicated by the fact that, to date, the mandate of Article 58 of the Personal Data Protection Act (PDP Act) regarding the establishment of a personal data protection authority has not been fully implemented, resulting in suboptimal oversight and enforcement of laws against personal data protection violations in the fintech sector. This study aims to analyze the reconstruction of a model for a personal data protection authority in the implementation of Article 58 of the PDP Law to strengthen consumer protection for PayLater fintech services, as well as to identify the factors that act as barriers to its implementation. The study employs a normative legal methodology using a legislative approach, a conceptual approach, and a comparative approach. Primary, secondary, and tertiary legal sources were analyzed using qualitative descriptive methods through a literature review. The research findings indicate that the implementation of Article 58 of the Personal Data Protection Act requires institutional restructuring through the establishment of the Personal Data Protection Authority as an independent, professional, and accountable state agency, with authority that includes risk-based oversight, compliance audits, review of Data Protection Impact Assessments (DPIAs), the application of the principles of "privacy by design" and "privacy by default," oversight of granular consent mechanisms, the enforcement of administrative sanctions, and integrated coordination with the Financial Services Authority (OJK) and other relevant agencies. This study also found that the implementation of Article 58 of the Personal Data Protection Law still faces various obstacles, including the failure to establish a personal data protection agency, delays in implementing regulations, overlapping authorities among agencies, limited human resources and digital oversight infrastructure, low personal data protection literacy, and the lack of a culture of compliance among fintech operators.

INTRODUCTION

Information and communication technology has driven significant transformation in the financial services sector in Indonesia. One form of innovation that is growing rapidly is financial technology (*financial technology* or *Fintech*), which offers a wide range of digital-based financial services with the characteristics of being faster, more practical, and more accessible to the public.¹ Among these various innovations, the PayLater service is one of the financing facilities that has experienced a significant increase in use. This scheme provides an opportunity for consumers to obtain goods or services first without making direct payments, then pay off these obligations through an installment mechanism within a certain period of time in accordance with the provisions that have been agreed between the parties.²

The existence of the PayLater service basically provides considerable benefits for the public, especially in increasing access to consumptive financing quickly without complicated procedures as commonly found in conventional financial institutions.³ In addition to providing convenience in the transaction process, this service also contributes to the acceleration of digital financial inclusion in Indonesia. However, these developments are inseparable from various legal consequences that require serious attention, especially related to the protection of consumers' personal data as one of the fundamental rights that must be guaranteed by the state.

In practice, the implementation of the PayLater service requires users to provide various personal information as part of the identity verification process and creditworthiness analysis. The data collected is not only limited to basic identity, but can also include phone numbers, email addresses, employment information, bank accounts, and access to contact lists on users' electronic devices.⁴ Such data collection in a wide scope increases the potential for misuse if it is not accompanied by adequate data protection governance and effective monitoring mechanisms.

¹ Hetty Hassanah and Wahyudi Wahyudi, "Legal Protection of Consumer Personal Data on the Use of Fintech in E-Commerce," *Jurnal Bina Mulia Hukum* 10, no. 1 (September 2025): 68–84.

² Benedict Guttman-Kenney, Chris Firth, and John Gathergood, "Buy Now, Pay Later (BNPL)... on Your Credit Card," *Journal of Behavioral and Experimental Finance* 37 (2023): 100788.

³ Audi Sonia Putri Maharani and Adi Suliantoro, "Consumer Protection in the PayLater Payment System Based on the Consumer Protection Law (Law No. 8 of 1999) in Indonesia," *Audi et AP: Journal of Legal Research* 5, no. 02 (2026): 222–35.

⁴ Megawati Agus Cristine, Frangki Mario Angelo Risakota, and Steffy Ruth Celine Sirait, "Protection of Personal Data in the Automatic Credit Scoring System by Fintech in Indonesia: Normative Juridical Analysis Based on Law Number 27 of 2022," *Journal of Modern Legal Studies* 7, no. 3 (2025): 1–15.

Various cases show that violations of personal data protection in *fintech* services still often occur.⁵ These forms of violations include the aggressive use of personal data for billing purposes, the dissemination of information about consumer debts to third parties, including family and emergency contacts without valid consent, and the occurrence of personal data leakage due to weak information security systems.⁶ This condition not only causes material losses in the form of potential identity abuse and financial losses, but also results in immaterial losses in the form of privacy disruptions, reputational damage, psychological pressure, and loss of sense of security for consumers in utilizing digital financial services.

In response to the increasing need for legal certainty in personal data protection, the government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).⁷ The presence of this law is a strategic step in building a comprehensive personal data protection system in Indonesia while adapting to the increasingly complex development of the digital economy. The PDP Law not only regulates the rights of personal data subjects and the obligations of controllers and processors of personal data, but also establishes an institutional framework that aims to ensure the effectiveness of supervision over all personal data processing activities.⁸

In this context, Article 58 of the PDP Law expressly stipulates that the implementation of personal data protection is carried out by the Government through an institution determined by the President. The regulation shows that lawmakers want an authority that has special authority to supervise the implementation of personal data protection provisions, enforce administrative laws, receive public complaints, resolve certain disputes, and ensure compliance with all controllers and processors of personal data,⁹ including *fintech* service providers and PayLater. The existence of these institutions is expected to be able to carry out the supervisory function independently, professionally,

⁵ Intan Audia Priskarini and Kukuh Tejomurti, "The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia," *Journal of Law* 6, no. 3 (2019): 556–75.

⁶ Angelia, Finesse Sly Oeijono, and Daniel Limbong, "Legal Protection of Paylater Users on E-Commerce Platforms for Personal Data Leakage," *Amnesty: Legal Journal* 6, no. 2 (2024): 174–85.

⁷ Bella Fistya Asherli and Sidi Ahyar Wiraguna, "Personal Data Security Protection in the Digital Era Facing Phishing Attacks Reviewed from the Personal Data Protection Law Number 27 of 2022," *Journal of Law, Public and State Administration* 2, no. 4 (2025): 1–14.

⁸ Catherine Wijaya et al., "Protection of Consumers' Personal Data in Digital Financial Services: A Review of the PDP Law," *Bureaucracy: Journal of Law and Constitutional Science* 3, no. 2 (2025): 30–42.

⁹ Juan Matheus and Ariawan Gunadi, "The Establishment of Personal Data Protection Supervisory Institutions in the Digital Economy Era: A Comparative Study with ICC," *JUSTICE* 10, no. 1 (2024): 20–35, <https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.

and accountably so that it can provide an effective guarantee of legal protection for the public as the owner of personal data.

However, until now the establishment of the institution as mandated in Article 58 of the PDP Law is still facing delays. This condition poses problems in the implementation of personal data protection because there is no authority that specifically carries out the function of supervision and law enforcement as referred to in the law.¹⁰ As a result, there is an institutional *vacuum* which has an impact on the suboptimal supervision of *fintech* companies' compliance in managing consumers' personal data. This situation has the potential to weaken the effectiveness of the implementation of the PDP Law, reduce legal certainty for the public, and limit consumers' access to quickly and effectively complaint and restoration mechanisms when there is a breach of their personal data. Therefore, accelerating the establishment of a personal data protection institution is an urgent need as part of efforts to realize a comprehensive legal protection system, increase the accountability of *fintech* service providers, and strengthen public trust in the digital financial ecosystem in Indonesia.

This study focuses on two main problems related to the effectiveness of law enforcement on personal data protection. How can the reconstruction of the model of personal data protection institutions be carried out in accordance with Article 58 of the PDP Law to strengthen the protection of *PayLater fintech* consumers in Indonesia? What are the factors that are obstacles when implementing Article 58 of the PDP Law that triggers the need to reconstruct the institution model to protect *consumers of PayLater* services?

METHODS

This research uses normative juridical research methods with an approach that relies on the analysis of primary legal materials and secondary legal materials, including laws and regulations, doctrines, legal theories, court decisions, and various relevant scientific literature. Data collection and analysis are carried out in a qualitative descriptive manner through the presentation of legal materials in the form of narrative descriptions to identify, study, and interpret the legal problems that are the object of research. This approach was chosen because it is able to provide a comprehensive understanding of the construction of legal norms, synchronization of laws and regulations, and legal concepts related to the formation of an institutional model of personal data protection.

¹⁰ Alex Maxer Pattipeilohy, Agus Satory, and Mahipal Mahipal, "Analysis of Paylater's Consumer Legal Awareness of Personal Data Based on Law No. 27 of 2022 concerning Personal Data Protection," *Journal of Social and Humanities* 5, no. 3 (2025): 4001-7.

Nevertheless, the characteristics of normative juridical research have the potential to cause subjectivity in the process of interpreting legal materials. Therefore, this study applies systematic analysis, consistent legal argumentation, and methodological transparency to minimize potential bias and increase the validity of research results.

RESULTS AND DISCUSSION

1. The reconstruction of the model of the Personal Data Protection Institution can be carried out in the implementation of Article 58 of the PDP Law to strengthen the protection of *fintech* paylater consumers in Indonesia

The reconstruction of the institutional model of personal data protection providers in order to implement Article 58 of the PDP Law is one of the fundamental needs in the development of the national legal system in the era of digital transformation. The reconstruction cannot be understood only as administrative changes or adjustments to the organizational structure of the government, but as an effort to reform institutions that have strategic value to answer the increasingly complex problems of personal data protection, especially in the implementation of *fintech* services, including the PayLater financing scheme. The development of the digital economy ecosystem has increased the intensity of the collection, storage, and processing of personal data by business actors, so an institution that has the capacity, authority, and independence is needed to ensure that all data processing activities are carried out in accordance with the principles of personal data protection regulated in laws and regulations.

The provisions of Article 58 paragraph (2) of the PDP Law expressly stipulate that the implementation of personal data protection is carried out by an institution determined by the President. This norm shows the will of the lawmakers to build an authority that is able to carry out the functions of supervision, guidance, and law enforcement of all personal data processing activities in Indonesia. The existence of this institution is expected to be able to be a meeting point between the interests of the state in maintaining legal order, the interests of business actors in obtaining regulatory certainty, and the interests of the public as the subject of personal data who are entitled to guarantee the security and confidentiality of their data. However, until now the mandate of the establishment of the institution has not been fully realized, so the implementation of the PDP Law has not run optimally. This condition has the potential to make the provisions of Article 58 only normative without being followed by the effectiveness of implementation in practice, which ultimately reduces the usefulness of the law as an instrument of legal protection for the community.

Based on these conditions, the reconstruction of the institutional model needs to begin with the construction of an institutional foundation that is able to guarantee the independence of the institution in real terms, both from the influence of political power and the economic interests of business actors. The author proposes the establishment of the Personal Data Protection Authority (OPDP) as a non-structural state institution that has an independent position and is accountable to the President within the framework of government administration. This accountability should not be interpreted as a form of subordination that opens up space for intervention in the implementation of the institution's duties and authority. Therefore, the institutional design of the OPDP must be equipped with *an effective checks and balances* mechanism so that functional independence is maintained.¹¹

One form of strengthening can be done through the selection mechanism of leaders or commissioners involving the House of Representatives as a representative of democratic supervision, by applying the principles of transparency, public participation, accountability, integrity, and professionalism in each stage of selection. In addition, the commissioner needs to be given a permanent term of office of five years with a dismissal mechanism that can only be carried out based on reasons that have been determined limitively in the laws and regulations. Such a model will provide institutional certainty while minimizing the potential for intervention from any party.

Strengthening institutional independence becomes even more important when it is associated with the characteristics of the *fintech* industry which is dominated by large-scale technology companies with economic capacity and very significant market influence. In practice, PayLater service providers manage millions of users' personal data that is a strategic asset of the company. The magnitude of these economic interests has the potential to create a conflict between the protection of consumer privacy rights and the company's business interests in utilizing data for various commercial purposes. The experience of various countries shows that data protection authorities that do not have institutional independence tend to have difficulties in carrying out their supervisory functions objectively and are less effective in cracking down on violations committed by large companies. Therefore, the establishment of OPDP as an independent institution is an important prerequisite for realizing a personal data protection system that is fair and oriented towards the public interest.

¹¹ Fatimah Hs et al., "Independence of Supervisory Institutions: The Key to the Effectiveness of Personal Data Protection Laws," *Zaaken: Journal of Civil and Business Law* 6, no. 2 (2025): 209–23.

In addition to strengthening institutional aspects, reconstruction also needs to be directed at expanding the functions and authority of institutions as stipulated in Article 59 and Article 60 of the PDP Law. So far, the function of personal data protection tends to be understood as limited to policy formulation and administrative supervision. In fact, the development of digital technology requires a more adaptive, preventive, and *risk-based approach (risk-based supervision)*. Therefore, OPDP is not only tasked with formulating national policies in the field of personal data protection, but must also have the authority to actively supervise all controllers and processors of personal data, especially in the *fintech* sector which has a high level of risk of violating people's privacy rights.

In the context of implementing the PayLater service, OPDP needs to be given the authority to ensure that each operator applies the principles of *privacy by design* and *privacy by default* from the system design stage to the operational implementation of the application. The application of these two principles aims to make the aspect of personal data protection an inherent part of the entire technology development process, not just an administrative obligation after the application is operational. As such, any features developed should be designed to minimize the collection of irrelevant data, limit access to personal information, and ensure that the initial setup of the system has provided users with the maximum level of privacy protection.

Furthermore, the consent mechanism provided by consumers also needs to be reconstructed to truly reflect the free will of the data subject. The practice of giving consent through a button or a checkbox (*generic consent*) without adequate explanation often causes consumers to not understand the scope of use of their personal data. Therefore, OPDP needs to require the use of a *granular consent* mechanism, which is consent given separately for each data processing purpose so that users have the opportunity to specify specifically what data can be processed and for what purpose the data is used. Such an approach will strengthen respect for the autonomy rights of data subjects while increasing transparency in the legal relationship between PayLater service providers and their consumers.

The reconstruction of the authority of the OPDP also needs to include the granting of authority to conduct periodic compliance audits and incidental audits of companies that are suspected of violations. In addition, institutions must be authorized to ask operators to compile and submit a Data Protection Impact Assessment (DPIA) as a form of evaluation of the risk of processing personal data before a system or service is operated. This authority will strengthen the prevention function so that potential violations can be identified early. In the event that violations are found, OPDP must have the authority to

impose administrative sanctions gradually and proportionately, ranging from written reprimands, temporary suspension of data processing activities, deletion of illegally processed data, to the imposition of administrative fines in accordance with the provisions stipulated in the PDP Law. The application of strict sanctions will provide a *deterrent effect* while encouraging the growth of a *compliance culture* among digital service providers.

Another aspect that is no less important in institutional reconstruction is the strengthening of coordination between state institutions that have authority in the field of supervision of the financial services sector. In this case, OPDP needs to build a structured cooperation mechanism with the Financial Services Authority (OJK), both through a *memorandum of understanding*, the establishment of a joint task force, and an integrated information exchange system. A clear division of authority will avoid overlapping supervision. OJK continues to carry out the function of regulating and supervising prudential aspects, financial system stability, and consumer protection in the financial services sector, while OPDP focuses on supervising the compliance of operators in managing personal data in accordance with the principles of personal data protection.

This synergy is very relevant in resolving various cases of personal data misuse on PayLater services, especially debt collection practices that are carried out by contacting family, friends, or emergency contacts of consumers without a valid basis for consent. In such a situation, coordination between OPDP and OJK will allow for faster, more comprehensive, and legal certainty for all parties. This approach not only strengthens the preventive legal protection function through increased supervision, but also increases the effectiveness of repressive legal protection through the enforcement of sanctions for violations that have occurred.¹²

In addition to institutional and regulatory aspects, the reconstruction of the model of personal data protection providers must also pay attention to the increasingly complex development of digital technology. The use of *big data* technology, *cloud computing*, and *artificial intelligence* has changed the pattern of personal data processing to be much faster and more massive than ever before. Therefore, OPDP needs to be supported by a technological infrastructure that is able to carry out digital surveillance in an ongoing manner, including the use of automated analysis systems to detect potentially unlawful data processing activities, identify data leakage patterns, and provide early warning of cybersecurity threats.

¹² Rahma Agri Firdaus, "Legal Protection and Prevention of Cybercrime in the Digital Era in the Legal System in Indonesia," *STAATSRECHT: Journal of Islamic State and Political Law* 4, no. 1 (2024): 79–104.

Strengthening the capacity of human resources is also an integral part of institutional reconstruction. OPDP needs to develop education, training, and certification systems for DPOs, especially in the digital financial services sector which has a high level of complexity in managing personal data. The presence of a competent DPO will help companies implement better data protection governance while ensuring that all data processing activities are in accordance with applicable legal provisions.

2. Factors that Become Obstacles in the Implementation of Article 58 of the PDP Law

The implementation of Article 58 of the PDP Law still faces various obstacles that are multidimensional.¹³ These obstacles are not only related to normative aspects in the form of incomplete implementation regulations, but also related to institutional issues, coordination between authorities, readiness of human resources, the development of digital technology, and the low level of public literacy regarding the right to personal data protection. The complexity of the problem shows that the effectiveness of the implementation of Article 58 of the PDP Law cannot be realized only through the existence of legal norms, but requires the establishment of an institutional system that is able to implement the provisions of the law consistently and sustainably.

Article 58 paragraph (2) of the PDP Law mandates that the implementation of personal data protection is carried out by an institution determined by the President. This provision is a manifestation of the need for a special authority that has the authority to supervise the processing of personal data, ensure the compliance of data controllers and processors, and provide legal protection to the public as the subject of personal data. However, until mid-2026, the formation of the institution in question has not been definitively realized. This condition creates an institutional *vacuum* that has a direct impact on the effectiveness of the implementation of the PDP Law, especially in the digital financial services sector which is growing very rapidly, including PayLater services.¹⁴ The absence of a authority that has full authority has caused the supervision, law enforcement, and complaint settlement mechanisms to not run optimally.

From the perspective of state administrative law, the existence of a norm without the support of an effective implementing institution will reduce the *effectiveness* of a law and regulation. In other words, the establishment of an institution as referred to in Article 58 is not just the implementation of the government's formal obligations to the mandate of

¹³ Muh. Arfhani Ichsan AH and Muh. Chaerul Anwar, "Urgency of Establishing an Independent Supervisory Body to Implement Article 58 of Indonesia's Data Protection Law," *Alauddin Law Development Journal* 8, no. 1 (2026): 7-17, <https://doi.org/10.24252/aldev.v8i1.67700>.

¹⁴ Gusti Ramadhani and Cecep Suhardiman, "The Impasse in the Establishment of Personal Data Protection Institutions and Its Implications on the Effectiveness of the PDP Law in Indonesia," *Journal of Social, Political and Humanities Research (JURRISH)* 5, no. 1 (2026).

the law, but is a fundamental prerequisite for the creation of a personal data protection system that provides legal certainty, justice, and benefits for the community. Therefore, the problems faced today cannot be seen as mere administrative delays, but rather reflect structural challenges in building personal data protection governance amid the acceleration of digital transformation.

One of the most influential factors on the suboptimal implementation of Article 58 is the lack of adequate implementing regulatory tools. Although the PDP Law has been in effect since 2022, a number of provisions that form the operational basis for the implementation of the law have not yet been fully formed. The absence of implementing regulations causes the division of authority, inter-agency coordination mechanisms, supervision procedures, procedures for examining alleged violations, and the mechanism for imposing administrative sanctions that do not have clear guidelines.¹⁵ As a result, various provisions in the PDP Law are difficult to implement effectively in practice.

The impact of these conditions is very much felt by consumers who use PayLater services. Not a few people experience the misuse of personal data in the form of the use of personal information in the debt collection process, the dissemination of identity to third parties, and the use of data outside of the approved purpose. When such violations occur, consumers often face difficulties in determining which institutions are authorized to receive complaints and provide legal remedy. Some of the complaints are directed to the OJK, others to the ministry in charge of digital affairs, while some aspects of information security are the domain of the State Cyber and Cryptography Agency. This fragmentation of authority causes the complaint handling process to take longer and often does not result in a settlement that provides legal certainty for victims.

In addition to regulatory barriers, institutional aspects are also problems that require serious attention. The institutional design to be built must be able to ensure the independence of personal data protection institutions so that they are able to carry out their supervisory functions objectively. Independence is an important principle in the implementation of the rule of law because it ensures that every decision to supervise and enforce the law is based on legal provisions, not on political interests or economic pressure. In the context of PayLater services, the need for independence is increasingly important considering that service providers are generally part of the ecosystem of large-scale digital technology companies that have a significant economic influence. Without a

¹⁵ Setyo Utomo, "Personal Data Protection Through Law Number 27 Of 2022: Challenges Of Cybercrime in The Era of Globalization and Digital," *Pena Justisia: Communication Media and Legal Studies* 23, no. 3 (2024): 2967-75.

guarantee of independence, the effectiveness of supervision of personal data processing practices has the potential to decline so that consumer rights are not optimally protected.

Another problem that hinders the implementation of Article 58 is the overlapping of authority between government agencies. Supervision of the digital financial services sector currently involves various institutions that have different authorities according to their respective fields of duty.¹⁶ OJK has the function of regulating and supervising financial services business activities, the ministry in charge of digital affairs is responsible for the implementation of electronic systems, while the State Cyber and Cryptography Agency plays a role in the national cyber security aspect. The division of authority is basically necessary, but without a clear coordination mechanism, it has the potential to cause duplication of supervision and a lack of responsibility in certain aspects. Such conditions not only harm the public as justice seekers, but also create uncertainty for business actors regarding the authorities that have the main authority in supervising the protection of personal data.

The next obstacle relates to the readiness of human resources and institutional capacity. Personal data protection is a field that is developing very quickly along with the advancement of information technology. Therefore, the implementation of the PDP Law requires apparatus that has competence in the fields of law, information security, data governance, digital audits, and artificial intelligence. The availability of professionals who have cross-disciplinary expertise is still relatively limited. On the other hand, not all *fintech* companies, especially small and medium-sized companies, have the financial or technical capabilities to build a comprehensive personal data protection compliance system. These limitations cause the application of personal data protection principles to often only be fulfilled administratively without substantial implementation.

Advances in digital technology also present new challenges that are increasingly complex. The use of *big data*, cloud computing, machine learning algorithms, and artificial intelligence allows the processing of personal data to be carried out in very large quantities and take place automatically. On the one hand, the technology provides benefits in improving the efficiency of digital financial services. However, on the other hand, the technology also increases the risk of data misuse, algorithm-based discrimination, information leakage, and data processing without legal consent. In such a situation, supervision that still relies on conventional mechanisms is no longer adequate. Institutions with technological capacity are needed to conduct digital

¹⁶ Dhea Cantik and Adhining Prabawati Rahmahani, "The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law," *International Journal of Science and Environment (IJSE)* 6, no. 1 (2026): 300–308.

monitoring, risk-based compliance audits, and early detection of potential violations before causing wider losses to the community.

In addition to institutional and technological factors, social aspects also have a considerable influence on the effectiveness of the implementation of the PDP Law. The level of public literacy regarding personal data protection still needs to be improved. Many users of the PayLater service do not understand their rights as data subjects, including the right to obtain information, the right to withdraw consent, the right to object to the processing of certain data, and the right to obtain compensation in the event of a violation. In the practice of using digital applications, people often immediately agree to the terms and conditions of the service without thoroughly reading the content of the agreement or privacy policy provided by the organizer. As a result, consent given is often not based on an adequate understanding of the legal consequences of the use of personal data.

On the other hand, some business actors still view compliance with personal data protection as an administrative burden that can reduce the company's operational efficiency.¹⁷ A business orientation that emphasizes more on user growth and economic benefits sometimes means that the aspect of data protection has not been placed as a top priority in corporate governance. These conditions show that the successful implementation of the PDP Law does not only depend on the existence of regulations, but also requires a change in legal *culture* that places respect for the right to privacy as part of responsible business practices.

In the perspective of national digital economy development, these obstacles have broader implications. Public trust is one of the main foundations in the development of the digital economy. If people do not get guarantees that their personal data is managed safely and responsibly, the level of trust in digital services will decrease. This decline in trust has the potential to hinder the growth of the *fintech industry*, reduce the competitiveness of Indonesia's digital economy, and affect the investment climate in the information technology sector.

From the perspective of the regulatory state, the development of the digital economy shows that the state no longer plays a role solely as a legal norm shaper, but also as a regulator tasked with creating an effective supervisory mechanism for increasingly complex economic activities. The characteristics of the financial technology industry that are rapidly evolving, based on technological innovation, and involving the processing of

¹⁷ Yusuf Daeng et al., "Personal Data Protection in the Digital Age: A Review of the Legal Framework for Privacy Protection," *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 2898–2905.

personal data on a large scale require an adaptive and risk-based supervisory model. Therefore, the existence of an independent personal data protection authority is part of the transformation of the modern state's functions to maintain a balance between digital innovation, economic interests, and the protection of people's fundamental rights. This argument is also strengthened by institutional design theory which emphasizes that the effectiveness of an institution is largely determined by its institutional design. Formal independence will not result in effective oversight if it is not supported by clear authority, accountability mechanisms, professional human resources, adequate funding, and good coordination with other institutions that have relevant authority. Thus, the institutional design of the Personal Data Protection Authority (OPDP) must not only guarantee normative independence, but also be able to create effective supervision and law enforcement in practice.

In addition, the development of digital transactions that increasingly involve cross-border data processing requires Indonesia to have a personal data protection system that meets international standards. The existence of an independent data protection authority with clear authority will increase Indonesia's credibility in international digital economy cooperation, including in cross-border data transfer mechanisms. Thus, the establishment of institutions as mandated by Article 58 of the PDP Law is not only important for the protection of citizens' rights, but also has strategic value in strengthening Indonesia's position in the global digital economy ecosystem.

CONCLUSION

The reconstruction of the model of personal data protection providers is an urgent need in realizing the implementation of Article 58 of Law Number 27 of 2022 concerning Personal Data Protection, especially to strengthen legal protection for consumers of PayLater financial technology services in Indonesia. The establishment of the institution as mandated in these provisions is not solely intended as a fulfillment of the normative obligations of the lawmakers, but as an institutional instrument that is able to ensure legal certainty, effective supervision, and law enforcement of all personal data processing activities. The dynamics of the rapid development of digital technology have increased the intensity of the collection, use, storage, and utilization of personal data by fintech service providers, so that the risk of violation of the right to personal data protection is also increasingly complex. In this context, the existence of an independent institution, having clear authority, adequate institutional capacity, and being supported by professional human resources is an important prerequisite for the realization of an

effective personal data protection system and able to provide legal protection guarantees to the public as data subjects.

Based on the results of the research, institutional reconstruction needs to be realized through the establishment of the Personal Data Protection Authority (OPDP) as a non-structural state institution that has functional independence, but remains in an accountable constitutional system. This independence needs to be guaranteed through a checks and balances mechanism, a transparent and competency-based leadership selection process, a term of office that provides legal certainty, and an accountability mechanism that keeps institutions free from political intervention and economic interests. In addition, the authority of the OPDP needs to be expanded so that it not only focuses on policy formulation, but also includes risk-based supervision, compliance audits, examinations of alleged violations, evaluation of Data Protection Impact Assessment (DPIA), supervision of the application of the principles of privacy by design and privacy by default, supervision of granular consent mechanisms, and the imposition of administrative sanctions that are effective, proportionate, and provide a deterrent effect.

Strengthening coordination with the Financial Services Authority (OJK), the ministry that handles government affairs in the digital sector, and the State Cyber and Cryptography Agency (BSSN) is also needed to build an integrated supervision system, so as to prevent overlapping authorities and gaps in the enforcement of personal data protection laws. Theoretically, this research contributes to the development of the legal study of personal data protection by offering an institutional reconstruction model that places the independence of supervisory authorities as the main prerequisite for the effectiveness of law enforcement in the digital economy sector. The model enriches the discourse on the relationship between institutional design, supervisory governance, and the protection of constitutional rights to personal data, especially in the PayLater financial technology service ecosystem which has high-risk data processing characteristics. From a practical perspective, the results of this research are expected to be considered for lawmakers and the government in drafting regulations for the implementation of Article 58 of the Personal Data Protection Law, including the establishment of OPDP along with institutional design, supervision mechanisms, and division of authority between authorities. In addition, the findings of this study can be a reference for fintech service providers in strengthening compliance with the principles of personal data protection and encouraging the creation of data governance that is more accountable and oriented towards the protection of data subject rights.

REFERENCES

- AH, Muh. Arfhani Ichsan, and Muh. Chaerul Anwar. "Urgency of Establishing an Independent Supervisory Body to Implement Article 58 of Indonesia's Data Protection Law." *Alauddin Law Development Journal* 8, no. 1 (2026): 7-17. <https://doi.org/10.24252/aldev.v8i1.67700>.
- Angelia, Finesse Sly Oeijono, and Daniel Limbong. "Legal Protection of Paylater Users on E-Commerce Platforms for Personal Data Leakage." *Amnesti: Jurnal Hukum* 6, no. 2 (2024): 174-85.
- Asherli, Bella Fistya, and Sidi Ahyar Wiraguna. "Perlindungan Keamanan Data Pribadi Di Era Digital Menghadapi Serangan Phishing Ditinjau Dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022." *Jurnal Hukum, Administrasi Publik Dan Negara* 2, no. 4 (2025): 1-14.
- Cantik, Dhea, and Adhining Prabawati Rahmahani. "The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law." *International Journal of Science and Environment (IJSE)* 6, no. 1 (2026): 300-308.
- Cristine, Megawati Agus, Frangki Mario Angelo Risakota, and Steffy Ruth Celine Sirait. "Perlindungan Data Pribadi Dalam Sistem Skoring Kredit Otomatis Oleh Fintech Di Indonesia: Analisis Yuridis Normatif Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Studi Hukum Modern* 7, no. 3 (2025): 1-15.
- Daeng, Yusuf, Nasri Linra, Atan Darham, Derry Handrianto, Risky Risandy Sianturi, Denny Martin, Rendy Pratama Putra, and Hendi Saputra. "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi." *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 2898-2905.
- Firdaus, Rahma Agri. "Perlindungan Hukum Dan Pencegahan Kejahatan Siber Di Era Digital Dalam Sistem Hukum Di Indonesia." *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2024): 79-104.
- Guttman-Kenney, Benedict, Chris Firth, and John Gathergood. "Buy Now, Pay Later (BNPL)... on Your Credit Card." *Journal of Behavioral and Experimental Finance* 37 (2023): 100788.
- Hassanah, Hetty, and Wahyudi Wahyudi. "Legal Protection of Consumer Personal Data on the Use of Fintech in E-Commerce." *Jurnal Bina Mulia Hukum* 10, no. 1 (September 2025): 68-84.
- Hs, Fatimah, Nursalam Rahmatullah, Hamsah Hamsah, and Hasmiati Hasmiati. "Independensi Lembaga Pengawas: Kunci Efektivitas Undang-Undang Perlindungan Data Pribadi." *Zaaken: Journal of Civil and Business Law* 6, no. 2 (2025): 209-23.

- Maharani, Audi Sonia Putri, and Adi Suliantoro. "Perlindungan Konsumen Pada Sistem Pembayaran PayLater Berdasarkan Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) Di Indonesia." *Audi Et AP: Jurnal Penelitian Hukum* 5, no. 02 (2026): 222–35.
- Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *JUSTISI* 10, no. 1 (2024): 20–35.
<https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.
- Pattipeilohy, Alex Maxer, Agus Satory, and Mahipal Mahipal. "Analisis Kesadaran Hukum Konsumen Paylater Atas Data Pribadi Berdasarkan Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Arus Jurnal Sosial Dan Humaniora* 5, no. 3 (2025): 4001–7.
- Priskarini, Intan Audia, and Kukuh Tejomurti. "The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 6, no. 3 (2019): 556–75.
- Ramadhani, Gusti, and Cecep Suhardiman. "Kebuntuan Pembentukan Lembaga Pelindungan Data Pribadi Dan Implikasinya Terhadap Efektivitas UU PDP Di Indonesia." *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora (JURRISH)* 5, no. 1 (2026).
- Utomo, Setyo. "Personal Data Protection Through Law Number 27 Of 2022: Challenges Of Cybercrime in The Era of Globalization and Digital." *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 23, no. 3 (2024): 2967–75.
- Wijaya, Catherine, Corrie Yemima Ilona, Cristin Rosa Gultom, and Sri Handayani. "Perlindungan Data Pribadi Konsumen Dalam Layanan Keuangan Digital: Tinjauan Dari UU PDP." *Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara* 3, no. 2 (2025): 30–42.