JOURNAL OF LAW AND ECONOMICS
E-ISSN: 2963-7937, P-ISSN: 2963-9204
Volume 4 Number 1, May 2025, pp 39-49.
DOI: https://doi.org/10.56347/jle.v4i1.240.

Legal Protection Analysis of Personal Data Breaches in Shopee Paylater Consumer Loan Transactions

Dewi Noviyanti [a*], Yuniwati [b], Suratno [c]
[a*,b,c] Business Law Study Program, Institut Informatika dan Bisnis Darmajaya, Bandar Lampung City, Lampung Province, Indonesia.

ABSTRACT
The widespread use of personal information in pay-later-based loan applications services reflects the vulnerability of digital security systems implemented by technology companies in Indonesia. Recently, several Shopee users reported being victims of such cases, claiming they never activated the paylater feature, yet their bank loan applications were declined due to poor credit records linked to SPayLater usage. While services like Shopee's SPayLater offer convenience, they also increase the risks of default and data breaches. Incidents such as improper debt collection practices and unauthorized access to ShopeePay balance reveal flaws in the platform's data protection and security measures. This underscores the need for in-depth research to strengthen legal safeguards for consumer personal data in Shopee's digital transactions. Findings indicate that SPayLater, as the data controller, holds the responsibility to collect, process, and protect consumer information throughout its lifecycle. Nevertheless, Shopee is perceived to have fallen short in fulfilling this duty, resulting in consumers suffering losses from unauthorized use of their data for loan applications. This situation highlights the urgency for more robust legal protections—both internally and externally to guarantee the protection of users' personal information. This research uses a normative legal research type with a descriptive research type. The problem approach uses a statutory approach with a case approach.

ARTICLE HISTORY
Received 15 May 2025
Accepted 25 May 2025
Published 31 May 2025

KEYWORDS
Online Loans; Shopee Paylater; Legal Protection.

ABSTRAK
Maraknya penggunaan informasi pribadi dalam layanan aplikasi pinjaman berbasis paylater mencerminkan rentannya sistem keamanan digital yang diterapkan oleh perusahaan teknologi di Indonesia. Baru-baru ini, beberapa pengguna Shopee melaporkan telah menjadi korban kasus tersebut, dengan alasan tidak pernah mengaktifkan fitur paylater, namun pengajuan pinjaman bank mereka ditolak karena catatan kredit yang buruk terkait penggunaan SPayLater. Meskipun layanan seperti SPayLater milik Shopee menawarkan kemudahan, layanan tersebut juga meningkatkan risiko gagal bayar dan pelanggaran data. Insiden seperti praktik penagihan utang yang tidak tepat dan akses tidak sah ke saldo ShopeePay mengungkap kelemahan dalam perlindungan data dan langkah-langkah keamanan platform tersebut. Hal ini menggarisbawahi perlunya penelitian mendalam untuk memperkuat perlindungan hukum atas data pribadi konsumen dalam transaksi digital Shopee. Temuan menunjukkan bahwa SPayLater, sebagai pengendali data, memegang tanggung jawab untuk mengumpulkan, memproses, dan melindungi informasi konsumen sepanjang siklus hidupnya. Namun demikian, Shopee dianggap telah gagal dalam memenuhi tugas ini, yang mengakibatkan konsumen menderita kerugian akibat penggunaan data mereka yang tidak sah untuk aplikasi pinjaman. Situasi ini menyoroti urgensi untuk perlindungan hukum yang lebih kuat—baik secara internal maupun eksternal untuk menjamin perlindungan informasi pribadi pengguna. Penelitian ini menggunakan jenis penelitian hukum normatif dengan jenis penelitian deskriptif. Pendekatan masalah menggunakan pendekatan perundang-undangan dengan pendekatan kasus.

KATA KUNCI
Pinjaman Online; Shopee Paylater; Perlindungan Hukum.

CONTACT Dewi Noviyanti dewi@darmajaya.ac.id Business Law Study Program, Institut Informatika dan Bisnis Darmajaya, Bandar Lampung City, Lampung Province, Indonesia.

1. Introduction

The swift advancement of technology and the push to offer additional value to debtors have led to transformations in the banking service system. Currently, banking activities and services to debtors have transformed from conventional models that are face-to-face and based on physical documents to digital-based services that no longer require direct meetings (Satyanegara *et al*., 2020). PayLater is a payment method that allows you to buy goods now and then pay for them later. Thus, if you have urgent needs, you can fulfill them first and pay when they are due. In Indonesia, the use of the PayLater platform has become an increasingly popular trend, especially among the digitally literate younger generation (Firdaus, 2023).

The results of a data survey conducted by the Katadata Insight Center (KIC) show that domestic PayLater users are dominated by Millennials and Gen Z. As many as 43.9% of PayLater users are from the Millennial generation, or those aged 26-35 years. Then, 26.5% of users are from Gen Z, or the 18-25 year age group (Mizanulhaq, 2024). Based on the latest survey, 21.3% of PayLater users are from the 36-45 year age group, showing a consistent increase from 18.9% in 2021 to 20.6% in 2022. This increase reflects the growing adoption of PayLater services among older users. The research team noted that this trend indicates increasing trust and comfort among users from this age group in utilizing digital financial services. In contrast, the lowest use of PayLater was recorded in the 46-55 age group (7.2%) and above 55 years (1.1%), which may be due to various factors, including traditional payment preferences or lack of digital literacy in this age group.

The advancement of electronic payment systems has triggered various changes. Technology and the internet have become essential in facilitating everyday human activities, significantly impacting various sectors—particularly the business sector. This influence has contributed to the growth of Indonesia's trade and financial industries, as evidenced by the rise of online trading and e-commerce. Along with the growth of e-commerce, the financial sector has also developed. In the e-commerce system, transactions between sellers and buyers are not carried out directly, so the payment method is usually done via interbank transfer or credit card. However, currently, in addition to these methods, a number of e-commerce business actors have also provided payment options in the absence of a credit card, referred to as the 'PayLater' method (Usman, 2017).

Globalization has a major impact on different areas of human existence, particularly in the evolution of technology and the internet. The presence of technological and internet advancements is a key component in assisting daily human functions, which then has implications for a number of sectors, especially business and industry. In Indonesia, one real manifestation of this influence is the rapid growth of the trade and finance sectors, marked by the emergence of a digital trading system or e-commerce. Developments in the trade sector are paralleled by significant progress in the financial sector. Within e-commerce, transactions occur remotely, with payments commonly executed via bank transfers or credit cards. However, in recent times, e-commerce players have also begun to offer alternative payment options without credit cards, namely through a delayed payment scheme known as PayLater. To prevent the possible misuse of personal information, the simplicity of e-commerce transactions should be balanced with stronger safeguards for consumer data against irresponsible parties. However, in its implementation, the PayLater payment system can actually become a loophole for cybercriminals to break into user accounts. One real example is the case of misuse of Shopee user data, which was used to apply for loans through the Shopee PayLater service. This incident shows that the consumer data protection system implemented by the service provider is still not optimal.

Furthermore, in situations of urgent need, the essential value of maintaining the confidentiality of consumer data in online buying and selling transactions becomes very real. One case that reflects this involves a leading e-commerce platform in Indonesia, namely Shopee. This platform offers an integrated mobile shopping experience with a live chat feature that facilitates interaction between sellers and buyers. Currently, various PayLater applications are available, and one that has been approved and is subject to supervision by the Financial Services Authority (OJK) is Shopee PayLater (SPayLater). This service is intended for Shopee users who meet certain criteria. In accordance with its function, SPayLater allows consumers to purchase products on the Shopee platform and make installment payments over a period of 1, 3, 6, or 12 months, according to the specified deadline. Several cases that have occurred show that consumers are often faced with the risk of privacy violations and unfair treatment in e-commerce transactions. Examples include billing practices that are not in accordance with the provisions and the unilateral activation of SPayLater services without consumer consent. These actions are inconsistent with Article 47 paragraph (1) of POJK Number 10 of 2022, which stipulates that consent must be obtained in advance from the owner of the personal data before using it. This situation emphasizes the importance of a more robust legal framework.

2. Methodology

This research adopts a normative legal method, chosen due to its relevance to the study's objective, which is to examine the regulatory framework concerning the legal protection of consumer data from misuse, particularly in relation to the Shopee PayLater feature (Benuf *et al*., 2019). This study employs an approach that combines both statutory and conceptual perspectives. To collect pertinent data and insights on the topics being analyzed, it utilizes primary legal resources, including laws related to personal data protection. Furthermore, it incorporates supplementary legal references such as textbooks, academic journals, scholarly articles, newspapers, theses, dissertations, and other academic publications that discuss the issue of personal data protection. The legal material collection technique used is library research, which involves gathering applicable primary and secondary legal materials related to the legal problems studied. These materials are then analyzed using theories that serve as a foundation in the research process. The analysis of legal materials in this study was conducted using a deductive approach. Legal materials obtained through literature studies were evaluated based on relevant legal issues, after which various alternative solutions to the problems were formulated. Additionally, the data was assessed according to applicable legal standards, and conclusions were drawn through a deductive method, emphasizing the importance of legal protection for consumer personal data. After identifying the norms governing the protection of these rights, the analysis proceeded to examine the form of legal protection for consumers who suffered losses due to the misuse of personal data in the Shopee PayLater service (Prasetyo, 2019).

3. Results

In its development, the use of the PayLater payment method does not always provide convenience. As the number of users continues to grow, potential risks also emerge, particularly from irresponsible parties who hack the accounts of e-commerce users who have activated the PayLater feature. There have even been cases where users who never activated the service still receive PayLater usage bills incurred by

others. Based on these cases, it is evident that the consumer data protection system in companies like Shopee still has weaknesses. Therefore, a more in-depth analysis of the agreement between the service provider and the consumer is necessary to examine the nature of the legal relationship established between the two parties and to identify which party bears responsibility for the misuse of personal consumer data, especially in the context of Shopee PayLater. In the PayLater service, there are generally three parties involved:

1) Account user, namely the Shopee account owner who uses the PayLater facility to make transactions and acts as a debtor.
2) E-commerce platform, as the PayLater service provider that offers various products or services.
3) Fintech company, as the lender that collaborates with Shopee to disburse funds and determine other lending provisions.

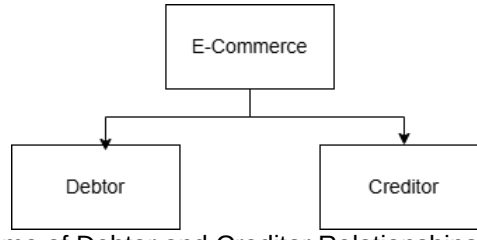

Figure 1. Scheme of Debtor and Creditor Relationships in E-Commerce

In the context of its role as a PayLater service provider, Shopee distributes loans through a partnership mechanism with an online lending company based on *peer-to-peer (P2P) lending*. Fintech companies operating online lending platforms are provided by non-bank financial institutions regulated by the Financial Services Authority (OJK), as stipulated in OJK Regulation Number 10/POJK.05/2022 on Information Technology-Based Joint Financing Services, particularly within the *peer-to-peer (P2P) lending* framework. Capital collected from investors is managed by the fintech provider and subsequently channeled to borrowers in need of funding. In the partnership between the e-commerce platform and the fintech company, the investors' funds are utilized to support transactions made by users through the PayLater feature.

1) The Concept of Personal Data Protection
   Personal data protection is a fundamental right aimed at ensuring the confidentiality, integrity, and availability of an individual's personal information. According to Solove (2008), personal data includes any information that can identify a person, and the misuse of such data can result in privacy violations, identity theft, and economic loss.
2) Applicable Legal Regulations
   In Indonesia, several laws and regulations govern the use and protection of personal data. Law No. 27 of 2022 on Personal Data Protection (PDP Law) is the first comprehensive regulation that recognizes the rights of data subjects and defines the responsibilities of data controllers and processors. Additionally, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016, emphasizes the importance of consent in the use of personal data (Article 26).
3) Previous Research on Data Breaches in Online Lending
   Several studies have addressed the issue of data breaches on fintech lending platforms. Rahmawati (2021) found that many online lending services in Indonesia do not implement adequate data protection mechanisms, particularly concerning the sharing of personal data with third-party debt collectors. Yustisia and Perdana

(2022) concluded that oversight by regulatory authorities remains weak, allowing unauthorized access and misuse of consumer data to persist.

The rapid development of digital technology has significantly altered financial behavior and consumer transaction patterns. One of the most prominent transformations is the rise of e-commerce and the adoption of electronic payment methods, including PayLater services. Shopee PayLater, as a digital financing feature integrated into the Shopee platform, enables consumers to make purchases with deferred payments. While this system offers convenience and flexibility, it also raises legal concerns regarding the protection of consumers' personal data. Despite regulatory efforts, such as the enactment of the Personal Data Protection Law (Law No. 27/2022) and earlier sectoral regulations like OJK Regulation No. 10/POJK.05/2022 on fintech lending, cases of data breaches and misuse in online loan and PayLater services continue to emerge. These include unauthorized access, third-party data sharing without consent, and aggressive debt collection practices using leaked personal data. This situation underscores the urgency of evaluating the effectiveness of current laws in safeguarding consumer privacy.

Previous studies have examined consumer protection in fintech (Benuf *et al*., 2019), regulatory frameworks, and general issues of e-commerce data privacy. However, few have focused specifically on the legal responsibility of e-commerce platforms in the context of PayLater data leaks. The lack of comprehensive legal analysis on the accountability of digital service providers in Indonesia represents a clear research gap. Moreover, compared to the *General Data Protection Regulation (GDPR)* in the European Union, Indonesia's regulatory framework is still developing in terms of enforcement mechanisms, institutional independence, and consumer remedies. This study aims to fill this gap by analyzing the legal accountability of Shopee PayLater service providers for personal data breaches and evaluating the adequacy of existing legal protections for consumers. By addressing these gaps, the research positions itself within the discourse on legal informatics, fintech regulation, and digital consumer rights protection. It also seeks to contribute comparative insights by examining international best practices.

4. Discussion

Based on the description of the PayLater service usage flow, it can be concluded that when a user registers and the service application is approved, the user is legally bound by an agreement with the PayLater service provider. This relationship takes the form of a service usage agreement, conceptualized as an electronic contract. According to Article 1, point 17 of Law No. 19 of 2016, which amends Law No. 11 of 2008 on Information and Electronic Transactions, an electronic contract is defined as "an agreement established between parties via an electronic system." This aligns with the definition in Article 1313 of the Civil Code, which describes an agreement as "an act where one or more persons bind themselves to one or more others." An agreement must be established freely, without any form of coercion or undue pressure from any party. Article 1320 of the Civil Code (KUHPerdata) further reinforces this principle by stating that an agreement is invalid if made under mistake, coercion, or deceit. In the context of utilizing PayLater services, the agreement is formed during the registration process, where users indicate their consent by checking a box, signifying acceptance of all applicable terms and conditions associated with the service. Key Elements of a Valid Agreement in PayLater Services

1) Competence Requirements
   This is fulfilled when the service user is declared to have passed verification based

on the submitted ID (KTP), confirming they meet the age requirements set by the service provider, which is between 21 and 70 years.

2) Specific Object
In the context of a valid agreement, this refers to the subject matter of the contract, which is the performance to be carried out—such as delivering something, performing an action, or refraining from doing something—as outlined in Article 1234 of the Civil Code. Performance represents the obligation of the debtor and the corresponding right of the creditor within the agreement. This condition is not met when the service user does not sign the electronic contract in the application. For instance, in cases of misuse of Shopee consumer data, none of the victims activated the Shopee PayLater feature, meaning they did not enter into an agreement with the PayLater service provider nor create an electronic contract.

3) Lawful Cause
A lawful cause means that the agreement is formed with a purpose that does not violate prevailing laws, legal prohibitions, or societal norms. This condition is considered fulfilled in the agreement for using the PayLater service as long as the contents of the agreement do not conflict with applicable laws and regulations. However, in some cases, consumers are harmed because they do not believe they have activated the PayLater feature, indicating they are not subject to the provisions set by Shopee (Fauziah & Santosa, 2024).

To further understand how this electronic agreement is formed, here is an illustration of the registration and activation process for the PayLater service on the Shopee application:

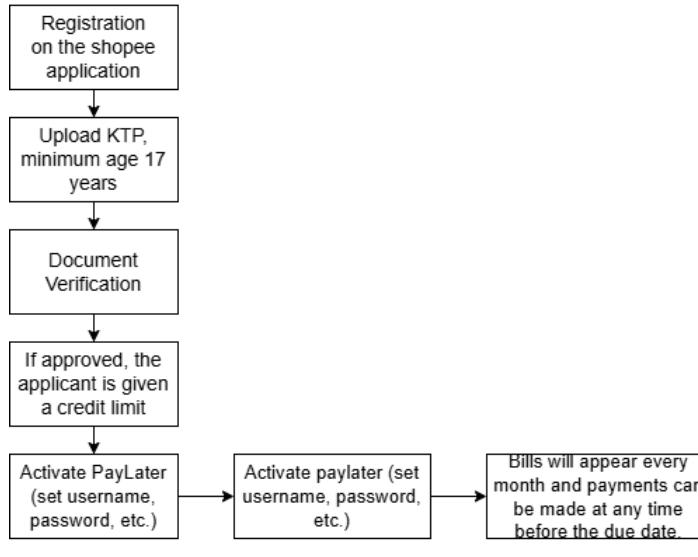

Figure 2. PayLater Registration and Activation Flow on the Shopee Application

The image above explains the steps that users must go through, starting from registering on the Shopee application, uploading an ID card with a minimum age limit of 17 years, verifying documents, to providing a credit limit if approved. After that, the user activates the PayLater feature by setting a username and password, and the bill will appear every month with payments that can be made at any time before the due date. Shopee sets terms and conditions regarding the responsibilities of account owners who have registered and provided personal data. These provisions prohibit account owners from providing access to other parties to use their accounts or transferring accounts to make transactions without Shopee's consent. These terms emphasize that use of the

account is at the owner's own risk, and Shopee is not responsible for any damage or loss caused by unauthorized use of the account. This regulation reflects the principle of personal data protection as stipulated in Law Number 27 of 2022 concerning Personal Data Protection. Clauses like those in Shopee's terms are known as exoneration clauses, which aim to diminish or abolish the accountability that the producer or business entity is expected to assume. Clauses of this nature clearly harm consumers, as they essentially force consumers to adhere to terms that predominantly favor business entities while disadvantaging them. Regulations regarding the use of standard clauses are outlined in Law No. 8 of 1999 on Consumer Protection, particularly Article 18 paragraph (1). This law places restrictions on business actors regarding the use of standard clauses in agreements. Specifically:

1) Article 18 paragraph (1) point (a) prohibits business actors from inserting standard clauses in contracts or related documents for goods or services that transfer their responsibility to consumers.
2) Article 18 paragraph (3) establishes that any such standard clauses included by business actors in the documents referred to in paragraph (1) shall be rendered legally void.

In light of this, the terms set by Shopee—which state that the platform bears no responsibility and that users cannot make claims for damages resulting from account hacking—clearly violate the provisions of the Consumer Protection Law. Although this law is titled the Consumer Protection Law, it addresses not only consumer interests but also the interests of business actors, as they determine the course of the economy. It is crucial to note that if business actors neglect to protect consumer personal data, they may also violate human rights. According to Jeanny Silvia Sirait, a public lawyer at the Jakarta Legal Aid Institute, regarding the online loan mechanism and consumer personal data, she stated, "Current online lending has actually violated Human Rights, both the Right to Privacy, the Right to a Sense of Security, and Economic, Social, and Cultural Rights (Consumer Rights)" (Jakarta Legal Aid Institute, 2021).

External legal protection ensures the safety of account holders by establishing laws aimed at preventing imbalances in technology-driven e-commerce transactions. In this context, the terms and conditions set by Shopee seek to regulate the rights and obligations of the parties in cases of account misuse, as outlined in Law No. 27 of 2022 on Personal Data Protection. However, these terms could potentially harm account holders. Accounts contain sensitive personal information such as names, passwords, identification details (including NIK), birthdates, residences, credit card numbers, and other private data that must be safeguarded and kept accurate within the electronic system. Protecting this personal data is crucial to maintaining its confidentiality and preventing cybercrimes, such as account misuse by malicious actors (Agus Sudibyo, 2019).

The spread of information creates privacy threats from parties who have access to a person's personal information. This means that PayLater service providers play a central role in protecting personal data as the party that receives and gains access to consumer data. While fintech companies generally deal directly with consumers in loan provision, in the case of PayLater, the electronic system organizer acts as a service provider in the form of a marketplace or e-commerce platform but also participates in running financial services based on fintech or through cooperation with third-party partners. In cases involving Shopee consumers, Shopee, as the controller of consumer personal data, should take an active role in preventing unauthorized access to personal data, as specified in Article 39 of the Personal Data Protection Law. One preventive action that should be implemented is providing a security system that can reliably, safely, and responsibly protect personal data processed in an electronic system.

If personal data protection is breached, the data controller must inform the data

subject and the relevant authority in writing within a maximum of 72 hours. The notification must include information regarding the disclosed personal data, when and how the data was disclosed, and the handling and recovery steps taken by the personal data controller. As stated in Article 46 of the Personal Data Protection Law, the personal data controller is accountable for managing personal data and must demonstrate responsibility if there is a failure to protect it (Article 47). Several cases have occurred involving Shopee account holders. For instance, on July 9, 2020, the owner of the account "arleen4_" received a call on behalf of Shopee, highlighting weaknesses in the security system and account management on the e-commerce platform. This incident demonstrates that consumers can become victims of fraud and data leaks, leading to financial losses and reduced trust in the e-commerce platform.

A contract in e-commerce is formed when the seller offers a form containing the terms of the contract, and the buyer agrees to the contents by checking a box or clicking the "accept" button as a sign of agreement. This action creates a deal between the seller and the buyer. E-commerce service providers are required to follow the standards applicable in their community and/or guidelines set by the government to ensure the provision of quality services. Generally, the organizer is fully responsible for all impacts of losses caused to other parties, although this responsibility can be limited if there is a specific mechanism used as a reference in best practices.

The Personal Data Protection Law No. 27 of 2022 reinforces the accountability of service providers to ensure the protection and security of consumers' personal information. They are required to implement an adequate security system to prevent illegal access, theft, or unauthorized use of data. Service providers must immediately respond to data leak incidents by closing existing security gaps and notifying consumers and authorities of the incident. The legal responsibility of service providers includes the obligation to provide compensation or damages if the data leak is caused by their negligence. To enrich the analysis, comparisons with other jurisdictions such as the European Union through the General Data Protection Regulation (GDPR) and California with the California Consumer Privacy Act (CCPA) are essential. The GDPR sets high standards for consent, data access and deletion rights, and imposes heavy administrative fines for violations (European Parliament and Council, 2016). For example, in the case of privacy violations by Amazon in Europe, the company was fined €746 million for failing to comply with the principles of lawful and transparent data processing (CNIL, 2021). When a data breach occurs, service providers are required to immediately halt data processing activities and inform affected consumers, as stipulated in Articles 46 to 49 of the Personal Data Protection Law. This responsibility includes not only data recovery efforts but also the protection of consumer rights and the prevention of further damage. Therefore, e-commerce platforms must comply with strict data protection standards and take full responsibility for any repercussions resulting from a data breach.

The establishment of a Personal Data Protection Supervisory Agency is intended to supervise and ensure the safety of electronic systems employed by companies in handling personal data, as per applicable legal standards. However, even with the enactment of the Personal Data Protection Law, the government has yet to establish this agency as an independent institution. Instead, as suggested by Article 58 of the law, it is positioned directly under the President, raising concerns about potential conflicts of interest or misuse for political purposes. Consequently, the agency operates within the governmental structure at the same level as other state institutions. This raises a critical question: can a government agency effectively impose sanctions on another agency within the same governmental hierarchy? (Muhtada & Diniyanto, 2021)

The analysis can be further enriched by applying Law and Economics Theory, which evaluates how data protection laws affect the behavior of economic actors. Without adequate sanctions or clear liability, platform providers may not invest sufficiently in

data security. In comparison, countries like Germany and South Korea have enforced robust data protection regimes with independent oversight agencies and clear consumer redress mechanisms. Indonesia could benefit from adopting similar institutional models. Although the Personal Data Protection Law (PDP Law) has been enacted, its enforcement mechanisms are still evolving. The absence of a fully operational Data Protection Authority delays effective oversight. Furthermore, the lack of mandatory breach notification to data subjects weakens the accountability framework. This stands in contrast to the EU's GDPR, which mandates breach notification within 72 hours and imposes heavy fines for violations.

The formation of an independent state institution is often motivated by public discontent with the effectiveness of existing agencies in managing new and evolving challenges. In light of repeated data breaches this year, numerous cases remain unresolved despite the intervention of the Ministry of Communication and Information. This is due to the absence of a dedicated agency to tackle this issue. Therefore, a personal data protection agency should be established as an independent entity to fill the gap in managing data protection concerns. Currently, placing the agency under the President's authority limits its ability to conduct thorough oversight. Indonesia should look to other countries with similar independent institutions for guidance in forming its own personal data protection agency.

5. Conclusion

As a service provider, Shopee is responsible for collecting, managing, and safeguarding consumer data throughout its lifecycle, from collection to destruction. However, Shopee's failure to protect consumer data led to losses, as personal information was misused to take out loans via the Shopee PayLater service. Therefore, legal protection for consumers is crucial, both internally and externally. Internal protection is reflected in the agreement between consumers and Shopee, which includes an exoneration clause that absolves Shopee of responsibility in case of data misuse, rendering the agreement legally invalid. On the other hand, external protection can be provided by imposing sanctions on Shopee as a data controller and processor under Law Number 27 of 2022 on Personal Data Protection. The objective of this study is to examine the legal protections for Shopee consumers in relation to the actions of service providers, offering suggestions for service providers to implement data protection strategies in line with the law, thereby ensuring the security and protection of consumer data from misuse.

Under the Consumer Protection Law, business actors have several responsibilities, including providing compensation for consumer losses, being accountable for their advertisements, and honoring the agreed-upon guarantees. These obligations are grounded in principles such as liability for negligence, strict liability, and the presumption of ongoing responsibility. E-commerce service providers must also comply with the provisions as stipulated in Law Number 27 of 2022 concerning Personal Data Protection obligates the protection of data privacy and the application of suitable data security measures management practices controls, and the assurance that the system remains secure against unauthorized access. These duties include protecting personal data, processing it legally, and ensuring transparency and accountability in cases of violations. By adhering to these personal data protection principles and legal obligations, service providers can foster consumer trust and better safeguard their rights. However, the enforcement of laws regarding consumer data breaches on Shopee's platform still faces challenges and shortcomings. Despite Shopee implementing various privacy policies to safeguard consumer data, the enforcement of existing laws remains insufficient.

References

Agus Sudibyo. (2019). *Liberation and control*. Gramedia Pustaka Utama.

Ashofa, B. (2004). *Legal research methods*. PT Rineka Cipta.

Benuf, C., Mahmudah, S., & Priyono, E. A. (2019). Legal Protection of Financial Technology Consumer Data Security in Indonesia. *Legal Reflections: Journal of Legal Sciences*, *3*(2), 145-160.

CNIL. (2021, July 30). Amazon fined €746M for GDPR violations. *European Data Protection Board*. https://edpb.europa.eu/news/national-news/2021/amazon-fined-eu746m-gdpr-violations_en

European Parliament and Council. (2016). *General Data Protection Regulation (EU) 2016/679*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

FAUZIAH, S., & SANTOSA, P. B. (2024). *Pengaruh Fintech Lending (Paylater) Dan E-Money Terhadap Perilaku Impulsive Buying Pada Generasi Muslim Z di Kota Semarang* (Thesis, UNDIP: Fakultas Ekonomika dan Bisnis).

Firdaus, N. A. (2023). *Tinjauan Hukum Islam Dan Peraturan Otoritas Jasa Keuangan Nomor 77/PJOK. 01/2016 Terhadap Praktik Pinjaman Shopee Paylater (SPayLater)* (Undergraduate (S1) Thesis, IAIN Ponorogo).

Marzuki, P. M. (2017). *Legal research*. Prenada Media Group.

Muhtada, D., & Diniyanto, A. (2021). Penataan Regulasi di Indonesia Melalui Lembaga Independen. *Pandecta Research Law Journal*, *16*(2), 279-291. https://doi.org/10.15294/pandecta.v16i2.31866

Prasetyo, T. (2019). *Legal research: A perspective of the theory of dignified justice*. Nusa Media.

Rahmawati, S. (2021). Consumer data privacy in fintech lending. *Jurnal Hukum & Regulasi Digital, 3*(1), 1–4.

Sabiq, F. (2022). PayLater reviewed from Law Number 11 of 2008 concerning Electronic Information and Transactions and Fatwa DSN-MUI No: 117/DSN-MUI/II/2018. *El-Hayah, 12*(1), 1–12. https://ejournal.uinsaid.ac.id/index.php/el-hayah/article/view/5461

Satyanegara, N., Priyono, J., & Paulus, D. H. (2020). Personal data protection in Indonesia in the context of electronic commerce (e-commerce). *Diponegoro Law Journal, 9*(2), 1–10.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Usman, R. (2017). Characteristics of Electronic Money in the Payment System. *Finance Review*, *32*(1), 89-96.

Yustisia, A., & Perdana, F. (2022). Legal protection of consumers in fintech services. *Jurnal IUS, 10*(2), 1–10.