International Journal of Research in Social Science and Humanities (IJRSS)

DOI: 10.47505/IJRSS.2025.8.2

E-ISSN : 2582-6220

Vol. 6 (8) August - 2025

Personal Data Protection in Digital Business Based on the Law on Personal Data Protection

Dony Dwi Wijayanto[1], Kadek Wiwik Indrayanti[2], & Diah Ayu Wisnu W [3]

[1-3]Master of Law Study Program

University Merdeka Malang

Indonesia

ABSTRACT

The development of information technology drives the growth of digital businesses in Indonesia, which directly increases the activities of collecting, processing, and storing consumer personal data. However, on the other hand, the rampant misuse and leakage of personal data pose a serious threat to the privacy rights of the public. The Indonesian government enacted Law Number 27 of 2022 on Personal Data Protection (PDP Law) as a legal framework governing personal data management, particularly within the digital business ecosystem to address this issue. This research uses a normative juridical method with a legislative and conceptual approach to analyze the regulation of personal data protection based on the PDP Law and the responsibilities of digital business actors in ensuring consumer rights. The research results show that the PDP Law has provided a sufficiently comprehensive legal framework for collecting, processing, storing, and deleting personal data. In addition, business operators must ensure data security, obtain consumer consent, and respect the rights to access and control personal data by data subjects. However, challenges still exist in implementing the PDP Law, particularly regarding the readiness of digital infrastructure, compliance by business actors, and law enforcement. Therefore, more optimal efforts are needed from both the government and business actors to realize adequate personal data protection and provide a sense of security to consumers in the digital business era. This research provides strategic recommendations in the form of enhanced education and training for business actors, strengthening the role of the Personal Data Protection Authority, and the development of cutting-edge data security technology as important steps in optimizing personal data protection in the digital business era.

Key Words: Business Responsibilities, Digital Business, Consumers, Law Number 27 of 2022, Personal Data Protection.

1. INTRODUCTION

The development of information and communication technology in the last two decades has significantly changed how humans interact and conduct economic activities (Amboro & Puspita, 2021). In Indonesia, the era of digitalization has driven the growth of a technology-based economy with the emergence of various forms of digital businesses such as e-commerce platforms, technology-based financial services (fintech), and transportation and food service applications. This condition creates significant opportunities for business actors to reach consumers widely, quickly, and efficiently. However, this progress also presents significant challenges, particularly in personal data collection and management (Anggitafani, 2020). Personal data has become a valuable asset for businesses and individuals. In the operations of digital businesses, entrepreneurs routinely collect and process sensitive information, such as names, addresses, phone numbers, financial data, and user consumption habits (Benuf et al., 2019). Unfortunately, many business operators still lack a strong understanding and commitment to maintaining the security and privacy of consumer data. This opens up opportunities for data breaches, information misuse, and illegal data trading practices that are detrimental to consumers (Dewi, 2016).

Indonesia has experienced several large-scale data breach incidents. One striking example is the data breach of Tokopedia platform users, which is evidence of the weak data protection in Indonesia. Before the enactment of Law

Number 27 of 2022 on Personal Data Protection (PDP Law), regulations related to personal data protection in Indonesia were still scattered across various sectoral rules that were weak in terms of legal standing and not uniform. This condition creates legal uncertainty, weak enforcement, and the absence of clear protection standards for business actors (Goeisepta et al., 2020). The government responded to the situation by enacting the PDP Law, a significant milestone in the national legal system in guaranteeing every individual's right to personal data protection (Hidayat et al., 2023). The PDP Law comprehensively regulates the rights of data subjects, the obligations of data controllers and processors, and administrative and criminal sanctions for violations. This law also introduces oversight by data protection authorities and dispute resolution mechanisms. In the context of digital business, the PDP Law positions business operators as personal data controllers responsible for managing data fairly, transparently, and accountably (Kusnadi, 2021).

Business operators must implement an adequate information security system and notify data subjects in the event of a breach. Failure to fulfill this obligation can result in severe administrative, civil, or criminal sanctions. The PDP Law explicitly regulates the types of personal data, including general and specific data, such as health and biometric data. Data subjects have the right to access, correct, delete data, and withdraw consent for data processing (Pratama et al., 2016). The obligations of data controllers also encompass aspects of security and transparency. The PDP Law prohibits the collection and use of data without permission and imposes sanctions in the form of fines up to IDR 6 billion or imprisonment for up to six years. Transparency is a key principle in the PDP Law, which requires data controllers to inform data subjects of the purpose of data collection, processing activities, and potential risks. This is usually conveyed through easily accessible and understandable privacy policies. In addition, the PDP Law also regulates the obligation of controllers to provide notification within 3x24 hours in the event of a data breach. The information must include the type of data leaked, the time and manner of the breach, and the recovery efforts undertaken. Accountability is another important aspect, where data controllers must be able to prove that they have processed data by applicable legal principles. Business operators must implement various security measures in daily operations such as strong passwords, two-factor authentication, data encryption, access control, system activity monitoring, and employee training.

These measures aim to minimize the risk of data misuse and build consumer trust. The PDP Law adopts principles from the European General Data Protection Regulation (GDPR), such as transparency, accountability, and purpose limitation. The PDP Law also applies to foreign entities that process the data of Indonesian citizens, demonstrating its broad legal reach. In digital business, compliance with the PDP Law becomes an important indicator for business sustainability. Business operators must obtain explicit user consent before collecting personal data, maintain data security from unauthorized access, and ensure the data is used for previously informed purposes. This legal compliance is important for protecting consumer rights and the reputation and sustainability of digital businesses in the era of information technology. With this background, it is important to thoroughly examine how the PDP Law's legal regulations protect personal data in digital business activities and to identify the legal responsibilities of business actors. This study is expected to provide legal and practical contributions to strengthening the legal awareness of business actors and protecting consumer rights in the digital world.

2. METHODOLOGY

The type of research used in this study is normative legal research, which is legal research conducted by examining library materials or secondary data and is often referred to as doctrinal research, where law is conceptualized as what is written in legislation (law in books) or as rules or norms that serve as guidelines for human behavior deemed appropriate. According to Peter Mahmud Marzuki, normative legal research is discovering legal rules, principles, and doctrines to address legal issues. This normative legal research aims to analyze legal norms, examine the conformity of regulations in the Personal Data Protection Law with digital business practices, and identify potential legal gaps or regulatory weaknesses in its implementation. The research approaches used include the statute approach and the conceptual approach. The statute approach is conducted by examining and reviewing all relevant laws and regulations related to the legal issue being studied, making it the methodological foundation for

DOI: 10.47505/IJRSS.2025.8.2

analyzing the written legal rules that are the subject of the study. Meanwhile, the conceptual approach is used by examining the views and doctrines developed in legal science to find ideas that align with the issues being studied.

3. RESULTS AND DISCUSSION

3.1 Legal Regulations Related to Personal Data Protection in Digital Business in Indonesia based on Law Number 27 of 2022 on Personal Data Protection

The foundation of consumer protection in Indonesian law is based on utility, justice, balance, consumer safety and security, and legal certainty. Consumer protection is part of the legal system aimed at creating governance of relationships between consumers and businesses in a fair, proportional, and sustainable manner (Priscyllia, 2019). The principle of benefit mandates that all forms of protection must bring advantages to all parties involved, both consumers and business actors (Puspita, 2023). Legal protection should not be biased in favor of one party, but must consider the principle of reciprocity in the trade and consumption of goods or services. In other words, consumer protection law is repressive towards violations and preventive against potential losses due to lack of information, production errors, or service discrepancies (Putri, 2018). The principle of justice in consumer protection aims to provide maximum participation space for the community within the national economic system. Consumers as legal subjects are entitled to information, comfort, safety, and compensation for losses suffered due to products or services that do not meet standards (Rahman, 2021). The principle of balance refers to the harmonious relationship between consumers, business operators, and the state. The state acts as a regulator and supervisor, businesses as providers of goods or services, and consumers as users who must be protected from irresponsible business practices. In this context, consumer protection has a dual purpose: to prevent the abuse of power by businesses and to empower consumers to advocate for their rights (Sautunnida, 2018) independently.

The principle of consumer safety and security is a form of legal responsibility towards a product's quality and safety standards. Goods or services in circulation must meet specifications that ensure consumer safety from health hazards, accidents, or damage. Certification bodies, production supervision, and administrative and criminal sanctions for negligent business operators reinforce these standards. The principle of legal certainty emphasizes that consumer protection must be within the legislative framework that can be effectively enforced. With regulations such as Law Number 8 of 1999 on Consumer Protection, consumers have a strong legal basis to assert their rights (Utomo et al., 2020). In considering the issuance of the Consumer Protection Law, the importance of increasing consumer awareness, knowledge, concern, ability, and independence to protect themselves from detrimental business practices is mentioned. The main objectives of consumer protection include: increasing consumer awareness and independence; elevating the dignity and status of consumers from negative access to products or services; enhancing consumer empowerment in choosing, determining, and demanding their rights; creating a transparent protection system and ensuring access to information; and fostering awareness among business actors to behave honestly and responsibly. This protection also encourages the improvement of product and service quality to maintain business continuity, consumer health, comfort, and safety (Yuniarti, 2019).

The existence of the Consumer Protection Non-Governmental Organization (LPKSM) plays a strategic role in overseeing business actors who pursue profit while neglecting product quality and safety. In practice, the Consumer Protection Law explicitly regulates the role and function of LPKSM in Article 44, which states that the government recognizes the existence of qualified LPKSM. LPKSM is given the space to actively participate in implementing consumer protection, including disseminating information to raise awareness of consumer rights and obligations, providing advice to consumers, collaborating with relevant agencies, advocating for consumer rights, and monitoring business practices that harm the community. LPKSM also plays a role in the legal process if a dispute arises between consumers and business operators. They can represent consumers in mediation processes, negotiations, and even in lawsuits in court. In addition, they promote public education and the development of legal advocacy for consumer rights. The challenges in implementing the role of LPKSM are limited resources, inaccessibility of remote areas, and lack of synergy with local governments. Therefore, strengthening institutional capacity, cross-sector collaboration, and regulatory support are important steps to enhance the effectiveness of LPKSM's role.

DOI: 10.47505/IJRSS.2025.8.2

In the framework of modern law, consumer protection is considered a complement to the trade system and a pillar of social and economic justice. The law should not only be present when disputes arise, but must also be proactive in shaping fair and civilized relationships between businesses and consumers. Thus, strengthening consumer protection through regulations, supervisory institutions, and community empowerment is an integral part of national legal development oriented towards the welfare of the people. Furthermore, in the context of globalization and the development of digital technology, consumer protection is experiencing new dynamics that demand regulatory adjustments. Consumers today not only interact directly in the buying and selling process but also through digital platforms that pose new risks such as online fraud, personal data breaches, and limited access to complaints. Therefore, consumer protection laws must be adaptive to the times. The state must encourage harmonization between consumer protection laws, cyber laws, and personal data protection to ensure that consumer interests are comprehensively protected.

In terms of supervision, synergy is needed between regulatory bodies such as the National Consumer Protection Agency (BPKN), LPKSM, and law enforcement officers to ensure that violations of consumer rights can be addressed firmly and swiftly. The existence of consumer courts, as a more straightforward and cheaper form of dispute resolution, needs to be better socialized to the public so that it can be maximally utilized. In addition, alternative dispute resolution mechanisms such as mediation and arbitration must be strengthened through supportive policies and facilities so that not all cases end up in court. In legal education, it is important to include consumer protection material in both formal and informal curricula. A legally educated society will be more aware of its rights, more critical in choosing products, and more active in voicing the injustices it experiences. This education is also part of the consumer empowerment strategy so that they do not only become objects of the law but also active subjects in maintaining the balance of legal relations with business actors. With strengthened regulations, synergy between institutions, and equitable legal education, consumer protection in Indonesia will become a normative slogan and a living practice in the daily lives of the community. Savvy consumers, responsible business operators, and a state that acts as a protector will create a healthy, fair, and sustainable economic ecosystem.

3.2 Analysis of Business Actors' Responsibilities in Providing Digital Business Protection Regarding Consumer Personal Data Protection

Digital business development in Indonesia has triggered a significant transformation in consumption patterns and the relationship between entrepreneurs and consumers. One of the most crucial aspects in this era is collecting and processing consumer personal data, which has now become a primary commodity. In this context, personal data is used not only for marketing purposes and consumer analysis but also for service development and optimization of digital business operations. Data has become a strategic asset that determines a business's sustainability and competitive advantage in the digital market. However, as data collection activities increase, the risk of personal data misuse also rises. Practices such as data breaches, identity theft, and the use of data without proper consent pose a real threat to consumer rights. Many cases show that consumer data is sold illegally or used for commercial purposes without transparency and accountability. This condition creates an urgency for strong and adequate legal protection to maintain the dignity and security of consumers as data subjects. In response to these challenges, Indonesia has enacted Law Number 27 of 2022 on Personal Data Protection (PDP Law), which explicitly regulates the rights and obligations of data subjects and controllers. The PDP Law provides a clear and comprehensive legal basis for regulating personal data processing activities, particularly in the digital sector. In this case, businesses acting as Personal Data Controllers have several legal responsibilities as follows:

a) Collecting and processing data based on legitimate legal grounds, including obtaining explicit consent from the data subject.

b) Providing clear, transparent, and accurate information to consumers regarding the purpose, types of data collected, and the data management process;

c) Implementing adequate technical and organizational measures to ensure the security of personal data from risks of leakage, manipulation, or illegal access.

DOI: 10.47505/IJRSS.2025.8.2

d) Ensuring the rights of data subjects, including the right to know, access, correct, delete, restrict, and withdraw consent for the processing of their data;

e) Being responsible for any losses the data subject suffers due to negligence, violation, or failure in managing personal data.

This responsibility has preventive and repressive dimensions. The preventive dimension emphasizes the obligation of business actors to design protection systems from the outset by applying the principles of "privacy by design" and "privacy by default." Meanwhile, the repressive dimension includes legal accountability in the event of violations that result in consumer losses, including the obligation to provide compensation or restitution. Although the PDP Law has been enacted, its implementation still faces various challenges. One of the main challenges is the weak data protection culture in digital business practices. Many business operators have not yet made data protection integral to their internal company policies. In several significant data breaches, such as on the e-commerce platforms Bukalapak and Tokopedia, the resolution has focused more on technical improvements to the security system without adequately compensating the affected consumers. This shows a gap between legal norms and the reality of practices. In addition to the responsibilities regulated under the PDP Law, business actors also must coordinate with supervisory agencies, such as the Ministry of Communication and Information (Kominfo) and the National Cyber and Crypto Agency (BSSN). Both are mandated to oversee the implementation of personal data protection policies and impose administrative and criminal sanctions on businesses that violate the regulations. The supervision carried out must be active, progressive, and risk-based to anticipate new threats that arise with technology development.

The urgency of establishing an independent personal data oversight agency is increasing, considering the complexity and dynamics of the digital sector. This institution will act as an authority that can swiftly and effectively address any violations and serve as a credible complaint center for the public. In addition, it is also important to establish an easily accessible and consumer-friendly dispute resolution mechanism, including alternative dispute resolution outside of court (non-litigation). From the consumer's perspective, the importance of education and digital literacy is inseparable from efforts to protect personal data. Consumers must understand their rights as data subjects, including giving valid consent, withdrawing consent, and accessing and correcting incorrect data. This education must be conducted on a massive scale through cooperation between the government, non-governmental organizations, academics, and business practitioners.

Furthermore, active participation from the community is also an important factor in social oversight of digital business practices. The collective awareness that personal data protection is a legal right will strengthen public pressure on businesses to be more responsible and transparent. This will create a healthy and sustainable digital ecosystem in the long term. Developing a code of ethics and conduct guidelines by digital business associations is no less important. By formulating internal ethical standards, businesses can foster a culture of voluntary and sustainable personal data protection. These guidelines will also help create accountability in the digital supply chain, from data collection to deletion.

Implementing the principles of "privacy by design" and "privacy by default" is a strategic step in ensuring that data protection has been an integral part of the technology architecture from the beginning of system design and not an afterthought. This includes strict access controls, data encryption, and regular information system audits. This principle also ensures that data is collected minimally and only to the extent necessary for specific services. In addition to strengthening laws and governance, economic incentives for companies that comply with data protection standards can also be an effective driver. The government can provide digital trust certifications, tax incentives, or preferential access to strategic projects for companies that have proven to protect their consumers' data well. This step will foster positive competition among businesses in terms of consumer protection. On an international scale, it is also important for Indonesia to align its personal data protection legal framework with global standards such as the European Union's General Data Protection Regulation (GDPR).

DOI: 10.47505/IJRSS.2025.8.2

This harmonization is crucial to strengthening the trust of international trade partners and opening up foreign investment opportunities in the digital sector. Thus, the responsibility of business actors is not only national but also meets global standards. In conclusion, protecting personal data is key to realizing justice and security within the digital economy ecosystem. Business actors as personal data controllers must bear comprehensive legal responsibilities, from preventive to repressive. Through regulation and supervision, the state must ensure that consumers' rights to personal data are truly respected and protected. On the other hand, consumers must continue to be empowered to advocate for their rights independently. Thus, Indonesia can build an inclusive, fair, and sustainable digital transformation with a strong foundation of legal protection.

4. CONCLUSION

Legal protection of consumer personal data in digital business in Indonesia has gained a strong foundation through Law Number 27 of 2022 on Personal Data Protection (PDP Law). This law provides legal certainty to consumers and requires digital business operators to implement the principles of transparency, security, and accountability in managing personal data. Business actors acting as Personal Data Controllers are obliged to collect and process data based on legitimate legal grounds, provide transparent information to consumers, and guarantee the rights of data subjects, including access, correction, deletion, and withdrawal of consent. These responsibilities are not only administrative but also encompass preventive and repressive aspects, with the threat of sanctions if violations or negligence occur that result in consumer harm. Although the legal framework is available, its implementation in the field still faces various obstacles, ranging from limited infrastructure and human resources to low legal awareness among business actors.

Cases of significant data breaches such as those that occurred on the Bukalapak and Tokopedia platforms indicate that most business operators have not fully internalized their legal responsibilities in personal data protection. Therefore, the effectiveness of personal data protection in the digital business sector must be supported by a layered strategy. The government needs to conduct extensive socialization and education for business actors and the public so that they understand their rights and obligations under the PDP Law. Strengthening institutions, especially the Personal Data Protection Authority, is also a strategic step in ensuring optimal supervision and law enforcement. On the other hand, business operators must enhance their internal capacity and awareness through the implementation of cutting-edge security technology, responsive data breach incident handling procedures, and privacy policies that are easily accessible and understandable. To create a climate of compliance, the government can provide incentives for compliant companies and strict sanctions for violators. In the long term, establishing a strong legal culture, collaboration among stakeholders, and developing industry ethical standards will be important foundations in building a consumer protection system based on personal data that is just, sustainable, and adaptive to the times.

REFERENCES

Amboro, F. Y. P., & Puspita, V. (2021). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). CoMBInES - Conference on Management, Business, Innovation, Education and Social Sciences, 1(1), 415–427. https://journal.uib.ac.id/index.php/combines/article/download/4466/1183

Anggitafani, R. F. (2020). Perlindungan Hukum Data Pribadi Peminjam Pinjaman Online Perspektif Pojk No. 1/Pojk.07/2013 tentang Perlindungan Konsumen Sektor Keuangan dan Aspek Kemaslahatan. Journal of Islamic Business Law, 5(2), 55–72. http://etheses.uin-malang.ac.id/25192/

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA KONSUMEN FINANCIAL TECHNOLOGY DI INDONESIA. Refleksi Hukum Jurnal Ilmu Hukum, 3(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Dewi, S. (2016). KONSEP PERLINDUNGAN HUKUM ATAS PRIVASI DAN DATA PRIBADI DIKAITKAN DENGAN PENGGUNAAN CLOUD COMPUTING DI INDONESIA. Yustisia Jurnal Hukum, 94. https://doi.org/10.20961/yustisia.v0i94.2780

DOI: 10.47505/IJRSS.2025.8.2

Goeisepta, A., Novera, A., & Mutiari, Y. L. (2020). PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN PADA FINANCIAL TECHNOLOGY (FINTECH) BERDASARKAN PERATURAN DAN PERUNDANG-UNDANGAN INDONESIA. https://repository.unsri.ac.id/34341/

Hidayat, T., Likadja, J. A. C., & Derozari, P. E. (2023). Perlindungan hukum data pribadi konsumen dalam perdagangan elektronik. Journal of Comprehensive Science (JCS), 2(5), 1087–1103. https://doi.org/10.59188/jcs.v2i5.323

Kusnadi, S. A. (2021). PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI. AL WASATH Jurnal Ilmu Hukum, 2(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Pratama, G. Y., Suradi, & Aminah. (2016). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PENGGUNA JASA TRANSPORTASI ONLINE DARI TINDAKAN PENYALAHGUNAAN PIHAK PENYEDIA JASA BERDASARKAN UNDANG-UNDANG NOMOR 8 TAHUN 1999 TENTANG PERLINDUNGAN KONSUMEN. Diponegoro Law Journal, 5(3), 1–19. https://ejournal3.undip.ac.id/index.php/dlr/article/view/12128

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi dalam Perspektif Perbandingan Hukum. Jurnal Jatiswara, 34(3). https://doi.org/10.29303/jatiswara.v34i3.218

Puspita, K. (2023). Perlindungan hukum data pribadi konsumen dalam perjanjian pinjaman online di Indonesia. Jurisprudensi Jurnal Ilmu Syariah Perundang-undangan Ekonomi Islam, 15(1), 67–83. https://doi.org/10.32505/jurisprudensi.v15i1.5478

Putri, M. S. (2018). Perlindungan hukum data pribadi bagi pelanggan jasa telekomunikasi terkait kewajiban registrasi kartu SIM. Jurnal Cakrawala Hukum, 9(2). https://doi.org/10.26905/idjch.v9i2.2772

Rahman, F. (2021). KERANGKA HUKUM PERLINDUNGAN DATA PRIBADI DALAM PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI INDONESIA. Jurnal Legislasi Indonesia, 18(1), 81. https://doi.org/10.54629/jli.v18i1.736

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. Kanun Jurnal Ilmu Hukum, 20(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159

Utomo, H. P., Gultom, E., & Afriana, A. (2020). URGENSI PERLINDUNGAN HUKUM DATA PRIBADI PASIEN DALAM PELAYANAN KESEHATAN BERBASIS TEKNOLOGI DI INDONESIA. Jurnal Ilmiah Galuh Justisi, 8(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Yuniarti, S. (2019). PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA. Business Economic Communication and Social Sciences (BECOSS) Journal, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030

DOI: 10.47505/IJRSS.2025.8.2