INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS)
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue XI November2025

Legal Protection for E-Commerce Consumers Against Personal Data Leaks

Muhammad Hasyim Maulana[1], Sodikin Sodikin[2]

[1,2]Faculty of Law, Universitas Muhammadiyah Jakarta, Indonesia

DOI: https://doi.org/10.47772/IJRISS.2025.91100329

Received: 21 November 2025; Accepted: 28 November 2025; Published: 10 December 2025

ABSTRACT

Legal protection for e-commerce consumers in the event of personal data leaks is crucial, as this data not only relates to individual privacy rights but also impacts aspects of state sovereignty. This study aims to analyze such legal protection, focusing on the implementation of Law Number 27 of 2022 concerning Personal Data Protection. The research addresses two main issues: first, the legal responsibilities of e-commerce businesses concerning personal data leaks, exemplified by the Tokopedia case in 2020; and second, the legal challenges associated with cross-border data transfers, which serve as the basis for a judicial review request to the Constitutional Court. The study employs a normative juridical method to examine the alignment of national legal norms with digital data management practices and the developments in international law. The findings indicate that while Law Number 27 of 2022 has strengthened the national legal framework, there are still gaps in supervision, law enforcement, and mechanisms for transferring data to foreign entities. This research aims to provide recommendations for the government, regulatory agencies, and businesses to enhance Indonesia's digital sovereignty and ensure the protection of consumer privacy rights.

Keywords: Legal Protection, Consumers, E-Commerce, Personal Data Leakage, Cross-Border Data Transfer.

INTRODUCTION

The development of digital economy in Indonesia has driven higher transactions using e-commerce as the main means of trade. With the tremendous growth of online transactions, personal information today is a strategic resource and extremely valuable commodity. This may be progress, but it has also exposed consumers to an increased potential for misuse of their personal data. One notable hack was the 2020 Tokopedia breach when the data of 91 million customers and 7 million merchants was leaked and then sold on the dark web. The case of this trouble, whose lawsuit is recorded as Decision Number 235/Pdt. G/2020/PN. Jkt. Pst in the Central Jakarta District Court (Hamid, 2025), **hig**hlighted the insufficient accountability of businesses in safeguarding personal data and the lack of specific regulations governing data protection at that time (V. A. Sari & Hanifah Febriani, 2025a).the inadequate responsibility of businesses in protecting personal data and the absence of certain regulations on data protection then (V. A. Sari & Hanifah Febriani, 2025a). As a result of court verdicts which have not given sufficient legal certainty to the consumer, the government promulgated Law Number 27 Year 2022 regarding Personal Data Protection (Sulistianingsih et al., 2023). The rights of data subject are guaranteed by this law; obligations of data controller are also the subject matter of it, and administrative and criminal sanctions for hampering the fulfilment of these rights have also been.

Implementation of the Personal Data Protection Law (PPDPA) has had major challenges such as the international flow of personal data. A lot of e-commerce companies in Indonesia use cloud services provided by companies based in other countries which causes the data collected to move out of the jurisdiction of Indonesia. This is one of the main reasons that this specific part of Law Number 27 of 2022 has been reviewed at the Constitutional Court for Case Number 137/PUU-XXIII/2025. The focus of the review was Article 56 (a rule regarding the treatment of personal data) which states that any data collected or processed must be done fairly and transparently. In order to ensure fair and just practices for managing personal data, people will need to have adequate access to make sure their rights are protected, and be able to hold other people accountable if their rights are violated (Aulia, 2024). The applicant argued that the provisions allowing for the transfer of

personal data outside of Indonesia may endanger digital sovereignty in Indonesia because there is no mechanism to do a transparent comparison of protection levels with countries outside of Indonesia where data may be sent. The applicant stated that there is an increased legal risk associated with the transfer of personal data to another country because not every country has the same standard regarding personal data protection.

This issue highlights that legal protection for digital consumers now encompasses not only individual privacy rights but also elements of state sovereignty. Law No. 27 of 2022, concerning Personal Data Protection, must effectively address cross-jurisdictional challenges so that Indonesia is not merely a user of technology, but also retains control over its citizens' data. By combining a normative analysis of laws and regulations with a case study of Tokopedia and recent developments in the Constitutional Court's judicial review, this study aims to provide a comprehensive overview of the effectiveness of consumer legal protection in the digital realm and to suggest ideal policy directions for strengthening national data sovereignty. From a social perspective, the digital era allows individuals to interact and conduct business with others across the globe with remarkable ease. This era enables transactions to take place without face-to-face contact, allowing purchases to be made even when business actors and consumers are geographically distant. Having the rule of law as a nation, Indonesia is supposed to have all kinds of activities including carrying out business operations within the confines of the law. Indonesia has consumer and business protection regulations, however, these regulations were made long before the digital age and as a result, they are unable to keep pace with the rapidly evolving activities of the people in the world today (Novita & Santoso, 2021).

The research focuses on the legislative safeguards for the protection of personal data in the context of e-commerce and applicable legislation such as Law Number 27 of 2022 on the Protection of Personal Data, especially regarding international data flows.

RESEARCH METHODS

This study analyzs consumer protection laws regarding loss of personal data via an e-commerce platform using a normative-descriptive method. Norms of Law Number 27 of 2022 is the norm from which this study is based. The study data is divided into three legal materials (primary, secondary, and tertiary). The legal materials which form the bulk of this study are primary legal materials which are authoritative and binding such as the Constitution, statutes, regulations, jurisprudence, and legal doctrines. These materials are legal and they are what law research seeks to address. Secondary legal materials are law books, articles of law, and research papers from which primary legal materials are analyzed. These are useful for the understanding of the legal documents constituting laws and regulations. Tertiary legal materials are legal encyclopedias, legal materials, legal commentaries of primary and secondary legal materials, legal e-publication, and newspapers. These materials have been useful to researchers as a basis for the legal issues they have researched. The analysis of the data (primary, secondary, tertiary legal materials) for this study is qualitative, adapted to the normative descriptive method.

RESULTS AND DISCUSSION

Implementation of Law No. 27 of 2022 on E-Commerce Consumer Protection

Law Number 27 of 2022 on Personal Data Protection (PDP Law) is the first of its kind in the national legal system, and it certainly will broaden the legal system on privacy rights and the legal protection on data in the digital world (Rosadi, 2023). Before, the protection of personal data was patchy and siloed in different sectoral laws. For instance, there was data protection in the laws in the field of Electronic Information and Transactions, and the laws of Consumer Protection. Such patchiness gave room for legal void and uncertainty because there was no standing legal framework that governs rights and obligations of businesses in controlling and processing personal data of their customers. Under the Consumer Protection Law, customers or consumers are defined as persons who use the goods and services available in the market for their own personal use or that of their family, others, or any other living being, for non-business purposes (Rosadi, 2023).

As of the enactment of Law Number 27 of 2022 regarding the Exemption of personal data protection, until

data, starting from the collection, storage, processing, and deletion of personal data. Also, this law is the first to explain and define the concepts of data controllers, data processors, and data subjects, which consist of various rights, such as the right to access, right to be forgotten, and right to withdraw consent. This regulation affirms the legal relationship of consumers as data owners and strengthens the legal position of consumers and drives businesses to implement the principle of precaution in the digital economic sector. These Electronic system operators must certify the electronic systems they manage, which they have to maintain the truth, validity, confidentiality, accuracy, and relevance, as well as the suitability for the purposes of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, disseminating, and destroying personal data, and must notify the personal data owners in writing of any breaches of the confidentiality of the personal data concerning the electronic systems they manage (Benuf et al. 2019)

Considering e-commerce activities, the influence of law number 27 of 2022 regarding personal data protection can be perceived by the fact that it specifies some duties that digital services providers are to perform regarding the protection of personal information. Every controller of personal data must adopt a reasonable security measure, perform data audits at regular intervals, and inform the supervisory authority and the affected data subjects of any breaches. This reflects the increasing number of breaches of privacy, such as Tokopedia breaches 2020, which saw millions of users data posted on illegal trading sites with no accountability on the company's part. Apparently Tokopedia had a major cyber attack wherein it was stated that there was a compromise of approximately 91 million users and 7 million merchant accounts as hacked, which was far greater than the 15 million that had been the subject of previous reports. Tokopedia was reported to have 91 million accounts as far back as 2019, with a later report by Suyanto (2013) saying that Tokopedia had 91 million accounts. This means that almost all of Tokopedia's accounts were part of the hacked accounts. The data that had been stolen, user ids, email addresses, full names, birth dates, gender, cell phone number, and unencrypted passwords and were sold on the dark web (Komalawati et al 2021).

Nevertheless, there are some institutional and technical challenges to fully implementing Law Number 27 of 2022 concerning Personal Data Protection. There is a lack of independent supervision as the Personal Data Protection Authority is still under construction and the supervisory functions still reside with the Ministry of Communication and Information Technology. This condition has caused overlapping of jurisdictions among institutions as well as the sluggish enforcement of the law on Personal Data Protection in the field of e-commerce. Moreover, there is a lack of comprehension among business practitioners about the provisions of Law Number 27 of 2022 concerning Personal Data Protection. Most e-commerce businesses do not have the adequate level of information security according to standards, and they consider privacy policies to be a mere bureaucratic legal document without even the means of authentication. This situation indicates that the provisions in Law Number 27 of 2022 concerning Personal Data Protection will not be fully effective because of the lack of functional digital infrastructure, effective manpower, and legal consciousness of the business community (Aulia, 2024).

To some extent, due to Law No 27 of 2022 about Personal Data Protection, consumers, in theory, have a stronger legal standing as entities that have control over their data. Nevertheless, consumers protection data still have issues with enforcement, administrative penalties, compliance of digital companies, and with Law No 27 of 2022 on Personal Data Protection Strength. L. E. Putri argues that there should be collaboration between responsible state authorities, tailored enforcement legislation, and an overall improvement in digital literacy of the citizens using e-commerce.

Legal Implications of Cross-Border Data Transfers on Indonesia's Digital Data Sovereignty

Due to advancements in digital technologies and the integration of global trading systems, the volume of cross-border data transfer has grown exponentially. As a result of the Personal Data Protection Act, Number 27 of 2022, the data transfer into and out of the country has grown. Most of the country's digital and e-commerce services run on data stored on the foreign-based cloud services. This situation creates challenges related to data and legal consumer protection, national security, and the protection of data and legal consumer protection. E-commerce has permeated all aspects of domestic and cross-border trade. Such realities underscore the rapid development of the convergence of IT, Telematics, and the emerging advancements of IT (Media and

Law Number 27 of 2022 concerning Personal Data Protection lays out the principles of cross-border data transfers in Article 56, which essentially allows the sending of individuals data to another country if that country has a comparable level of data protection to that of Indonesia (Aulia, 2024). However, to date there is no formal mechanism in place to assess this supposed comparability. Thus, the transfer of data across borders is a free for all with no mechanisms in place to track and monitor data subject rights abuse. One of the fundamental problems that arise is the lack of such a mechanism, which leaves a huge gap in the legal framework. In international regulations, such protective mechanisms are referred to as the adequacy decision component of the European Union (GDPR) regulation, which Indonesia unfortunately lacks. This has resulted in a situation where a huge number of commercial enterprises transfer data based purely on commercial contracts with no legal scrutiny to ensure the protection of the data belonging to Indonesian citizens.

Weak oversight has resulted in concern surrounding the implementation of Article 56 of Law Number 27 of 2022, and has thus resulted in a petition seeking a writ of certiorari to the Constitutional Court of Aulia (2024). There has been an infringement of the "sovereignty of the nation's data" due to the participation of foreigners in the management of the personal data of the citizens of Indonesia". There is also concern that the provisions on the transfer of data under the provisions of the Law Number 27 of 2022 lead to the absence of measures that provide an assessment of the level of data protection that is available, and that there are no measures that provide a basis to account for data protection that has been made accessible to foreign citizens. In the realm of the law, a law that is clearly drafted and enacted may be regarded as containing "legal certitude". In this regard, even though there could be a divergence in the perception of the law, the degree of certainty is very low in respect of the coherence and the rationality of the provisions. Such a situation is a fertile ground for the emergence of greater discord with what is regarded as the socio-legal order. Such phenomenon is what Utrecht describes as the theory of legal certainty, "Legal cognition is twofold, the existence of a rule of law that is general in nature, this is what legal knowledge is, and the individual needs to be informed with regard to the conduct that is legally acceptable and also the conduct that is deemed illegal, and the individual needs to be afforded legal protection against the exercise of arbitrary power by the state".

Based on the information available by October 2023, generally speaking, the protectionist nature of state practice as indicated in Article 56 of Law Number 27 of 2022 (Aulia, 2024). Nonetheless, at the practical stage, Indonesia, on the other hand, has profound difficulties in exercising supervision and control of the enforcement of the laws and regulations. The data protection authority defacto created by law has and continues to be sub-optimally established, thus, the sate of control of data that is exported and imported is at best, declarative and administrative. Such a state of affairs results in an adverse effect of Indonesia's weak bargaining position in the sphere of international cooperation in the digital economy (Geraldo, 2022).

Another important concern is the possible infringement of the rights of data subjects as a result of data processing, which is outside the territorial limits of the nation-state. In situations where there is a relocation of the personal data of Indonesian consumers to foreign servers, there is a relative ease in undertaking legal action for breach of privacy because of the disparity in legal frameworks, jurisdictions, and protection levels. In this scenario, affected consumers are deprived of access to effective legal redress, while there is a loss of control of the state over the circulation of information which is of great value to national security and other priorities (Bainus & Rachman, 2018). In addition, the practice of cross-border data transfers creates an uneven playing field between local and foreign enterprises. Foreign legal entities are said to possess better security arrangements and are compliant with laws, while local legal entities are said to be facing a greater burden in terms of complying with costly data protection measures. Such disparity is said to undermine the national ability to compete and worsen the dependency of Indonesia to foreign digital systems (Prabowo & Sihaloho, 2023).

When it comes to public policy, the problem of cross-border data transfers poses certain political economy and digital sovereignty challenges as well. These data transfers have strong implications for domestic data protection, as they will likely prompt Indonesia to adopt or strengthen certain protective data governance policies to mitigate the risks associated with cross-border data flows. With cross-border data transfer implications, Indonesia is likely to strengthen its data protection and privacy governance tailored to the cross-border transfer of data. This shows the importance of Indonesia strengthening legal data protection governance

in the context of cross-border data transfers. As data is strategic, governance poses risks to consumer protection, national cybersecurity, and the integrity of the country's digital sovereignty (Wulandari et al, 2024)

Legal Responsibility of E-Commerce Business Actors for Consumer Personal Data Leaks

Aspects of the e-commerce ecosystem have e-commerce ecosystem transformed the nature of the legal relationship between business actors and consumers. Beyond transactional relationships involving the purchase of goods and/or services, a further legal relationship has developed which involves the management of consumers' personal data which has both economic and privacy value (Nurani et al 2023). This management of data involves collection, storage, analysis, utilization for business purposes (e.g., profiling, personalization), and circulation to third parties, which all have the potential to leak and misuse data. This study seeks to establish the extent to which e-commerce businesses are liable for data leaks and what legal mechanisms, if any, are available to protect consumers. These issues must be addressed and analysed to determine to what extent e-commerce businesses are liable for the data leaks of consumers. .

Changes in the Legal Position of Business Actors: From Sectoral Regulations to Law Number 27 of 2022 Before implementing Law No. 27 of 2022, there were no consolidated, sectoral, comprehensive, and unified regulations regarding data privacy. There were only government regulations, presidential regulations, and ministerial regulations, which only caused confusion in determining the limits of the data controller's responsibility. Law No. 27 of 2022 provides a comprehensive and substantive development in which the data controller and data processor concepts are defined, regulates the rights of data subjects, and specifies the technical and administrative responsibilities of the controller and processor (Pohan & Nasution, 2023). This normative structure delineates the liability of business practitioners to victims of data breaches and the breach of the duty to protect data, notify, and provide access to remedies.

Before implementing Law No. 27 of 2022, there were no consolidated, sectoral, comprehensive, and unified regulations regarding data privacy. There were only government regulations, presidential regulations, and ministerial regulations, which only caused confusion in determining the limits of the data controller's responsibility. Law No. 27 of 2022 provides a comprehensive and substantive development in which the data controller and data processor concepts are defined, regulates the rights of data subjects, and specifies the technical and administrative responsibilities of the controller and processor (Pohan & Nasution, 2023). This normative structure delineates the liability of business practitioners to victims of data breaches and the breach of the duty to protect data, notify, and provide access to remedies.

Forms and Dimensions of Legal Responsibility of Business Actors

The legal responsibility of business actors for data leaks can be mapped into three complementary dimensions (Umboh, 2018):

1. Administrative obligations. The ability to use administrative sanctions (issues of warnings, administrative fines, restrictions of actions, and even repealing the ability to manage data) if violations of the requirements of technical or procedural compliance have been detected. The able sanctions for such administrative violations serves to quickly neutralize and provides the ability to quickly correct the misalignment of the company's practices.
2. Civil liability. A damages compensatory mechanism to the consumers/victims of the data leaks for the damages incurred, regardless of the material or intangible suffering. Civil liability needs to be substantiated for a breach of duty, negligence, or breach of the duty of contract of the data protection provisions; however, such violations have been often extremely difficult to prove only for intangible damages and causality able to be established digitally.
3. Criminal liability. For the actions which constitute the elements of a crime, for example, intentional data breach and data transactions of a criminal nature. The criminal provisions are punitive, thus they are clearly of a greater measure of proof required, greater commitment of resources of personnel to undertake the actions of the law enforcement authorities. In the practice, the ideal of the three ways of such provisions ought to be, and indeed ought to be, a combination of all of such three wherein the primary

liability also to compensate the victim, and of criminal liability of a combination of both for the intentional actions and the commercialization of the lost data. The existing deficiencies however ought to be noted such as the existence of a fragmented enforcement power for there is not yet a fully operative cohesive supervisory authority, the gap of inter agency coordination is substantial, and the violators are often only subject to prolonged and inadequate civil processes.

Obstacles to Proof and Measure of Compliance

1. Difficulty of technical proof. When a breach occurs there are numerous sources the breach could come from (corporate mistakes, mistakes from a third party, or high-level hacking). Digital forensics take time, and even when there are server logs, access histories, and security audits, those pieces of evidence are usually not kept or are hard to come by during litigation (Umboh, 2018).
2. Take it or leave it contracts. Limitations of liability clauses are included in the terms and conditions of many sites and are accepted by consumers without negotiation that leaves the consumer to suffer weaker civil claims (Eleanora & Dewi, 2022).
3. Standards of due diligence vary. Other than a few scant prescriptive national standards there are no regulations that require e-commerce platforms to create specific standards for things like level of encryption, how frequently audits are to be conducted, and what certification schemes should be used. This results in a wide range of standards that can be considered due diligence when it comes to a courts judgement. Jurisdictional fragmentation. If data is processed on offshore servers, litigation and sanctions enforcement encounters jurisdictional obstacles and lacks international willingness. Hence, the focus of assessing liability usually shifts from whether a breach occurred to how far the data controller went in terms of reasonable breach prevention and breach mitigation to an acceptable set of standards. This shifts the focus to compliance and prospective control measures (Zahwani & Nasution, 2024.

Recovery Mechanisms, the Role of Third Parties, and the Tokopedia Case

E-commerce businesses must ensure that data breaches are not only prevented, but that victims receive restitution, and that protection systems are bolstered throughout the entire data management chain. After a breach, businesses are legally and ethically bound to have prompt, effective, and transparent steps that provide remediation. This remediation can take the form of notification to the impacted data subjects; payment of damages if the amounts are considerable; and free identity theft and cybersecurity services to data breaches (Muhammad & Nugroho, 2021a). On the other hand, in civil advocacy, the process takes so long and is so costly that advocacy is ineffective. As a result, the victims cannot get justice without a lengthy process; victims of data breaches should have access to other administrative remedies such as mediation or fast arbitration before a data protection authority. These are not unreasonable as a set of regulations based on the Personal Data Protection Law should stipulate the timelines and forms of compensation that data controllers owe on breaches (Muhammad & Nugroho, 2021b). Conversely, e-commerce companies typically make use of a number of third parties, including providers of cloud storage, payment processing services, and data analysis systems. In this regard, legal responsibility continues to lie with the data controller, as the party that first defines the ends and means of personal data processing. Hence, the security clauses of such contracts with third parties must meet at least certain levels, should include obligations for data breach reporting, audit rights for the data controller, and fallback clauses that give the data controller the right to counterclaim against the third party for negligence. Gaps in such clauses risk the creation of legal silos that narrow the breach of legal relations for consumers. Considerable weakness in the corporate responsibility system prior to the implementation of Law No. 27 of 2022 can be illustrated with the Tokopedia data breach incident of 2020. Over 91 million users' information was leaked and sold in illicit online marketplaces, but respondents in the corporate legal responsibility system were virtually untouchable due to the absence of law for victims and the role of bystanders, particularly, third parties. Inaction on protecting consumer data nexus limitations on holding businesses accountable, as delineated in the Central Jakarta District Court Decision No. 235/Pdt.G/2020/PN.Jkt.Pst (V. A. Sari & Hanifah Febriani, 2025b). Following the enactment of Law No. 27 of 2022, the structuring of legal liability mechanisms is now possible. Data controllers report and notify data subjects of their breach, facing possible administrative, civil, or criminal liability. In the case of digital corporations, this is a paradigm shift from ex-post liability to ex-ante preventive and corrective liability.

Corporations are now required to possess internal recovery procedures (incident response plans), implement comprehensive data protection policies, and formalize contracts with external entities to guarantee enduring data protection (Aji, 2023). Thus, victim redress, third-party regulation, and the Tokopedia case precedents balance each other to illustrate the e-commerce sector's integrated liability. Protecting digital consumers legally is no longer a matter of substantive law only; having a real system in place with accountability, transparency, and user safety and fairness should be the focus.

Types of Licensing and Legal Approvals

In the provision of e-commerce services in Indonesia, licensing is a crucial legal element to Protecting personal data concerns while necessary must also be administered along with preventative measures to ensure the safe and ethical handling of consumer personal data (including):

1. Electronic System Provider Registration According to the Minister of Communication and Informatics Regulations (Permenkominfo) Number 5 of 2020 About Private Electronic System Organizers (T.B. Putri et al. 2025) Every e-commerce site is obligated to register as an Electronic System Provider (ESOP), and this registration serves as an Administrative Permit which ensures that an electronic system is able to satisfy the requirements of security, data governance, and with a clear and accessible privacy policy. The registration is done online via the Online Single Submission (OSS) system and it is mandatory to include technical documents, privacy policy, data security system, and location of the documents (servers). This obligation also applies to foreign entities that provide services to the public in Indonesia if they are processing the personal data of Indonesian citizens. Consequently, the registration of ESOP is the foremost legal instrument to enable the state to exercise control over the collection and processing of data by digital entities. Consent to Transfer of Personal Data Abroad Article 56 of Law Number 27 of 2022 stipulates that the transfer of personal data abroad may only occur if the destination country has protection standards equivalent to those of Indonesia. In this context, every e-commerce business using an overseas server is required to obtain approval from a data supervisory authority before conducting cross-border transfers. This approval includes an assessment of the level of protection, a post-transfer oversight mechanism, and a guarantee of a binding data protection agreement between entities (Widjaja, 2025). This mechanism is crucial because many Indonesian e-commerce platforms use cloud-based storage owned by foreign companies. Without adequate oversight, the risk of data leakage outside national jurisdiction could increase significantly.
2. Information Security Audit and Certification Obligations. As a form of preventative protection, companies must complete electronic system audits every so often. These include checking standards of encryption, access management, and system integrity. External, and government-recognized institutions, like ISO/IEC 27001 or national security certifications, also provide security certification for businesses that handle large amounts of data. This certification is often the bare minimum and a necessity to demonstrate legal culpability for a data breach but also acts to validate real technical compliance. Companies that do not possess security certification can be considered to have committed negligent breaches of the accountability principle as contained in Article 35 of Law Number 27 of 2022 (Kusuma 2023)
3. Data Subject Consent Data Subject Consent Although lacking authority of administrative consent, data subject consent has strong legal significance. This type of consent involves personal legitimation. Thus, consent should be given, consciously, purposefully, and explicitly. In e-commerce activities, collection, storage, or processing of personal data should be preceded by user consent through an unequivocal opt-in procedure. Consequently, the absence of legally valid consent may lead to damaging administrative or legal liability. Therefore, businesses have an obligation to design user consent processes with simple language and the ability to revoke consent easily (Clifford et al., 2019).
4. The combination of business permits, the Electronic System Operator registration, and adherence to Law Number 27 of 2022 shows the first example of policy synergy between digital economy and consumer protection as law. The government, through the Ministry of Communication and Information, the Financial Services Authority, and the National Cyber and Crypto Agency, is expected to improve coordination in the licensing of controllers of financial data and online transactions. In addition, integrated supervision of operational permits for e-commerce will ensure abuse of data management will build trust of the society on the e-commerce system of the country. The unified system will induce businesses to

adopt the measures of transparency, accountability, and responsibility in personal data management regulation (K. A. Sari, 2023)

Researcher's Contribution to Regulatory Gaps in the Implementation of the Personal Data Protection Law

The researcher proposes a strategic plan and implementation schedule for legal compliance that may serve as an operational model for business actors and controllers in response to the lack of technical guidelines on Personal Data Protection by Law Number 27 of 2022. The contribution of this proposal to the novelty of the research is that there is no integrated design linking the normative requirements of the PDP Law with the real implementation phases of an organization.

First, researchers emphasized that internal privacy policies need to match the data controlling and processing guidelines set out in the PDP Law. The guidelines for short-term alignment are necessary because many businesses have not yet developed internal standards that comply with the new regulations.
Second, this research highlights the urgency of appointing and certifying a Data Protection Officer (DPO). While regulations mandate the presence of a DPO, they do not provide clear implementation steps. Therefore, this research develops a realistic timeline to enable organizations to improve accountability and oversight of data processing.

Third, the researchers highlighted that the actual regulatory gap included relationships with third parties, such as cloud providers and payment gateways. While the PDP Law assigns joint responsibility, it does not detail any contractual mechanisms. In order to fill this gap, the research developed recommendations concerning the renewal of the cooperation agreement as part of data breach risk management.

Next, to ensure the sustainability of compliance, periodic audit and evaluation stages were proposed by the researcher. Because audit standardization has not been detailed within the regulations so far, the need for annual internal evaluations as a control against the effectiveness of data protection policies was formulated by the researcher.

This research also introduces the notion of an integrated data breach incident reporting system, something that has not been operationally outlined in the PDP Law. This model fills in a procedural gap, especially concerning response speed and in relation to transparency with the public.

Moreover, they gave long-term recommendations on data center consolidation in Indonesia to enhance digital sovereignty by preventing unauthorized data transfers, an aspect normatively regulated within the PDP Law but not technically elaborated.

Finally, the research provides a framework for legal compliance training and privacy awareness among all employes as a strategy for building a sustainable data protection culture. This approach widens the scope of the PDP Law, which to this day only highlighted the formal obligations of data controllers but has not addressed internal education aspects in detail.

Thus, this description shows that the research not only describes the obligations in the PDP Law but also fills in the implementation gap through designing a work plan, an implementation schedule, and an operational model applicable by various institutions. This adds value (novelty) and provides a substantial contribution to the research regarding data protection governance development in Indonesia.

CONCLUSION

Establishing comprehensive personal data protection governance from the government is yet another building block to ensure the public trust in Indonesia's digital economy. The government, in this case from the Ministry of Communication and Informatics, the Financial Services Authority, and other relevant supervising institutions needs to assess to what extent every e-commerce business practitioner respects the duties of a data controller, the principles of transparency, and accountability as in Law Number 27 of 2022 concerning

Personal Data Protection. The Tokopedia data breach and the litigation of Article 56 of Law No. 27 of 2022 indicate that the personal data protection scope is beyond technical measures that relate to digital sovereignty and cross-border legal liability. Thus, in relation to the legal protection of e-commerce consumers, there should be a legal perspective that places the government as the policy maker, and as the order giver, that supervises to ensure the business complies with the data protection laws.

Also, integrated supervisory mechanisms, augmented human resource capacity, and the exercise of due diligence by companies when working with third parties should accompany the proposed strengthening of Indonesia's Legal Personal Data Protection System (LPDPS). Increased digital security, legal clarity and assurance, consumer protection, and enhanced Indonesia digital sovereignty, and the development of a balanced and inclusive digital economy shall be achieved with the incorporation of the suggested due diligence principles.

REFERENCES

1. Aji, D. B. P. (2023). Protection of Personal Data in Online Transactions Study of Decision Number 235/Pdt. G/2020/Pn. Jkt. Pst.
2. Aulia, E. (2024). Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dari Perspektif Kepastian Hukum. UNES Law Review, 7(1), 220–227. https://review-unes.com/index.php/law/article/view/2267
3. Bainus, A., & Rachman, J. B. (2018). Kepentingan Nasional dalam Hubungan Internasional. Intermestic: Journal of International Studies, 2(2), 109–115. https://intermestic.unpad.ac.id/index.php/intermestic/article/download/74/34
4. Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. Refleksi Hukum: Jurnal Ilmu Hukum, 3(2), 145–160. https://ejournal.uksw.edu/refleksihukum/article/view/2413
5. Clifford, D., Graef, I., & Valcke, P. (2019). Pre-formulated declarations of data subject consent—Citizen-consumer empowerment and the alignment of data, consumer and competition law protections. German Law Journal, 20(5), 679–721.
6. Eleanora, F. N., & Dewi, A. S. (2022). Pelaksanaan Perjanjian Baku dan Akibat Hukumnya bagi Konsumen. Jurnal Mercatoria, 15(1), 19–27. https://ojs.uma.ac.id/index.php/mercatoria/article/view/6812
7. Geraldo, V. (2022). Kerja Sama Indonesia-Singapura Di Bidang Ekonomi Digital Melalui Pembentukan Kawasan Ekonomi Khusus Nongsa Digital Park Di Batam (2018-2020). Jurnal Ilmu Hubungan Internasional LINO, 2(2), 128–142. https://ojs.unsulbar.ac.id/index.php/lino/article/view/1746
8. Hamid, M. G. F. (n.d.). Penyelesaian Sengketa Konsumen di Platform Tokopedia (Studi Putusan 235/Pdt. G/2020/Pn. Jkt. Pst). Retrieved 19 November 2025.
9. Komalawati, D., MR, M. D., & Kartika, R. D. (2021). Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data. ., 2(1), 49–56. https://jurnalsyntaxadmiration.com/index.php/jurnal/article/download/167/249
10. Kusuma, S. C. B. (2023). Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [PhD Thesis, Universitas Islam Sultan Agung Semarang]. http://repository.unissula.ac.id/id/eprint/31440
11. Muhammad, M. O., & Nugroho, L. D. (2021a). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi. Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo, 14(2), 165–174. https://journal.trunojoyo.ac.id/pamator/article/view/12472
12. Muhammad, M. O., & Nugroho, L. D. (2021b). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi. Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo, 14(2), 165–174. https://journal.trunojoyo.ac.id/pamator/article/view/12472
13. Novita, Y. D., & Santoso, B. (2021). Urgensi pembaharuan regulasi perlindungan konsumen di era bisnis digital. Jurnal Pembangunan Hukum Indonesia, 3(1), 46–58. https://ejournal2.undip.ac.id/index.php/jphi/article/view/10233

14. Nurani, E., Wiryanto, W., & Riyanto, S. (2023). Optimalisasi Perlindungan Konsumen Atas Kebocoran Pengelolaan Data Pribadi Dalam Pinjaman Online. Jurnal Hukum Jurisdictie, 5(2), 51–69. https://dev-ojs.journalfhuia.ac.id/Jurisdictie/article/view/133
15. Pohan, T. D., & Nasution, M. I. P. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce. Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen, 1(3), 42–48. https://e-journal.nalanda.ac.id/index.php/SAMMAJIVA/article/view/336
16. Prabowo, T. B., & Sihaloho, R. A. (2023). Analisis ketergantungan indonesia pada teknologi asing dalam sektor energi dan dampaknya pada keamanan nasional. Jurnal Lemhannas RI, 11(1), 72–82. https://jurnal.lemhannas.go.id/index.php/jkl/article/view/426
17. Putri, L. E. (2023). Pengaruh E-Commerce Terhadap Perkembangan Usaha Di Indonesia. JURNAL TAFIDU, 2(1), 42–52.
18. Putri, T. B., Dewi, S., & Priowirjanto, E. S. (2025). Aspek Hukum Praktik Penghapusan Akun Pengguna Sistem Elektronik Secara Sepihak untuk Memoderasi Konten Oleh Marketplace Menurut Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat. JURNAL HUKUM, POLITIK DAN ILMU SOSIAL, 4(1), 10–27. https://ejurnal.politeknikpratama.ac.id/index.php/jhpis/article/view/4550
19. Rosadi, S. D. (2023). Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022). Sinar Grafika.
20. Sari, K. A. (2023). Integrasi Hukum Perlindungan Konsumen Dan Persaingan Usaha Atas Data Pribadi Konsumen Pada Platform Digital. UNES Law Review, 6(1), 1936–1947. https://www.review-unes.com/law/article/view/954.
21. Sari, V. A., & Hanifah Febriani, S. H. (2025a). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam e-Commerce (Studi Putusan Nomor 235/Pdt. G/2020/PN. Jkt. Pst) [PhD Thesis, Universitas Muhammadiyah Surakarta]. https://eprints.ums.ac.id/id/eprint/132219
22. Sari, V. A., & Hanifah Febriani, S. H. (2025b). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam e-Commerce (Studi Putusan Nomor 235/Pdt. G/2020/PN. Jkt. Pst) [PhD Thesis, Universitas Muhammadiyah Surakarta]. https://eprints.ums.ac.id/id/eprint/132219
23. Sitorus, S. Y. H. (2023). Perlindungan Hukum Data Pribadi Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Ditinjau dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi [PhD Thesis, Universitas Kristen Indonesia]. http://repository.uki.ac.id/11540/
24. Sommaliagustina, D. (2018). Perlindungan hukum terhadap konsumen e-commerce di Indonesia. Journal Equitable ISSN, 2541, 7037. http://download.garuda.kemdikbud.go.id/article.php?
25. Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). Masalah-Masalah Hukum, 52(1), 97–106. https://ejournal.undip.ac.id/index.php/mmh/article/view/51319
26. Suyanto, M. (2003). Strategi Periklanan pada E-commerce Perusahaan Top Dunia. Penerbit Andi: Yogyakarta.
27. Umboh, A. (2018). Tanggung Jawab Pelaku Usaha Dalam Pemenuhan Hak Konsumen Menurut Hukum Positif Indonesia. Lex Privatum, 6(6). https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/21498
28. Widjaja, G. (2025). Pengaruh Perjanjian Perdagangan Internasional Terhadap Kebijakan Perlindungan Data Pribadi. Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 4(4), 345–354. https://publish.ojs-indonesia.com/index.php/SIBATIK/article/view/2659
29. Wulandari, S. A., Aliyah, K. K., Faradilla, A. N., & Agustina, S. A. (2024). Implikasi Hukum Privasi Data Internasional terhadap Pilihan Konsumen dalam Penggunaan E-Commerce Lintas Negara. Indonesian Journal of Social Sciences and Humanities, 4(2), 82–87. http://journal.publication-center.com/index.php/ijssh/article/view/1739
30. Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. Journal of Sharia Economics Scholar (JoSES), 2(2).https://ojs.unimal.ac.id/joses/article/view/17122