priviet lab.
RESEARCH & PUBLISHING

Priviet Social Sciences Journal

Volume 6
Issue 5 May, 2026

Article 10

07-05-2026

Personal data protection in e-commerce platforms: Legal challenges, regulatory frameworks, and the path toward digital consumer trust

Inggret Adu

To cite this article: Adu, I. (2026). Personal data protection in e-commerce platforms: Legal challenges, regulatory frameworks, and the path toward digital consumer trust. *Priviet Social Sciences Journal, 6*(5), 118–128. https://doi.org/10.55942/pssj.v6i5.1815

To link to this article: https://doi.org/10.55942/pssj.v6i5.1815

Priviet Social Sciences Journal
E-ISSN 2798-6314
P-ISSN 2798-866X
https://doi.org/10.55942/pssj.v6i5.1815

Volume 6
Issue 5
May Edition 2026

Personal data protection in e-commerce platforms: Legal challenges, regulatory frameworks, and the path toward digital consumer trust

Inggret Adu

Faculty of Law, Social Sciences, and Political Science, Universitas Terbuka, Indonesia
email: 057483412@ecampus.ut.ac.id

Received 22 April 2025
Revised 27 April 2026
Accepted 07 May 2026

ABSTRACT

The proliferation of e-commerce platforms has fundamentally transformed how individuals engage in commercial transactions, generating immense volumes of personal data in the process. While this digital shift offers considerable economic benefits, it simultaneously exposes consumers to escalating risks of data misuse, unauthorized access, and identity theft. This article examines the legal and regulatory landscape governing personal data protection within e-commerce environments, drawing upon a qualitative literature review methodology. The study traces the evolution of global data protection frameworks—most notably the European Union's General Data Protection Regulation (GDPR)—and situates Indonesia's Law No. 27 of 2022 on Personal Data Protection (UU PDP) within this international context. Key findings indicate that while comprehensive legislation has been enacted in many jurisdictions, enforcement gaps, low organizational compliance, and technological complexity continue to undermine consumer data security. Empirical evidence from major data breaches between 2018 and 2024 illustrates the severity and frequency of vulnerabilities inherent in e-commerce ecosystems. Expert commentary and scholarly analysis further underscore the need for harmonized, principle-based regulation supported by robust institutional architecture. This article argues that effective personal data protection in e-commerce requires not merely legislative enactment but a sustained commitment to enforcement, digital literacy, and cross-border regulatory cooperation. Recommendations are directed at policymakers, platform operators, and legal scholars engaged in the evolving field of digital consumer rights.

Keywords: personal data protection; e-commerce; GDPR; UU PDP; data breach; digital consumer rights; privacy law

1. INTRODUCTION

The digital economy has grown at a pace few could have anticipated two decades ago. E-commerce platforms, ranging from global giants such as Amazon and Alibaba to regional platforms like Tokopedia and Shopee in Southeast Asia, now serve as the primary marketplace for billions of consumers. According to IBM (2024), the average global cost of a data breach reached USD 4.88 million, the highest figure ever recorded, underscoring the financial gravity of inadequate data protection systems (IBM Security, 2024). For e-commerce specifically, retail security incidents rose from 725 in 2023 to 837 in 2024, a 15% increase that signals a worsening threat environment (ISAC, 2024).

At the heart of this vulnerability lies personal data. Every transaction on an e-commerce platform involves the collection of sensitive information: names, addresses, payment credentials, browsing behavior, and purchase histories. These data points are not merely administrative records—they are assets, both to businesses seeking behavioral insights and to malicious actors seeking financial or reputational gain. The question of who is responsible for protecting this information, and under what legal framework, has therefore become one of the central questions of contemporary information law.

This article addresses that question through a structured academic inquiry. It examines existing legal frameworks, analyzes significant data breach incidents, considers expert perspectives from law and computer science scholarship, and evaluates the current state of Indonesia's data protection regime as a case study in emerging-economy compliance.

While prior scholarship has examined the GDPR–UU PDP comparison in general terms, a specific gap remains in the literature: the structural enforcement deficit within the e-commerce sector itself, existing studies tend to evaluate data protection frameworks at the legislative level without adequately interrogating why enforcement mechanisms fail specifically for e-commerce operators—a context defined by multi-party data supply chains, high MSME participation, and rapid technological change. This article addresses that gap by situating legal analysis within empirical evidence of breaches and governance critique, advancing the core argument that legislative enactment alone is insufficient without a sector-specific enforcement architecture and sustained institutional capacity.

Electronic commerce emerged as a commercial phenomenon in the 1990s, initially celebrated for its capacity to transcend geographic barriers and reduce transaction costs. The legal frameworks that governed commerce at the time—grounded in contract law, consumer protection statutes, and telecommunications regulations—were ill-equipped to address the unique characteristics of digital data flows. Personal information, once collected in physical form and stored in filing cabinets, now moves across national borders in milliseconds, processed by algorithms, shared with third-party vendors, and sometimes sold without the knowledge of the individuals to whom it belongs.

The foundational concern for data protection in commercial contexts is not new. As early as 1980, the Organisation for Economic Co-operation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, establishing eight core principles, including collection limitation, data quality, purpose specification, and individual participation, that would later inform national and regional legislation worldwide (OECD, 2013). Yet it was not until the European Union enacted the General Data Protection Regulation (GDPR) in 2016, applicable from May 2018, that a comprehensive and enforceable international standard emerged.

The GDPR represented a paradigmatic shift. By establishing individual rights (including the right to erasure, the right to data portability, and the right to object to automated decision-making), imposing obligations on data controllers and processors, and threatening fines of up to 4% of global annual turnover, the GDPR forced multinational companies to treat data protection as a legal and commercial imperative rather than an optional best practice. In the years following its implementation, other jurisdictions including Brazil, South Korea, and Indonesia (UU PDP, 2022), enacted their own comprehensive frameworks, many of them inspired by the GDPR's structure.

Indonesia's digital commerce environment provides a particularly instructive context. With over 200 million internet users and a rapidly expanding e-commerce market, Indonesia has experienced several

high-profile personal data breaches that exposed the vulnerabilities of both private platforms and public agencies. The enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP) marked a watershed moment for the country's approach to digital rights—but as subsequent sections of this article will demonstrate, enactment is only the first step.

2. LITERATURE REVIEW

2.1. Conceptual Foundations of Personal Data Protection

Scholars of information law have long distinguished between two competing visions of data protection. The first treats privacy as a fundamental human right, grounded in constitutional dignity and autonomy. This perspective, championed by theorists such as Westin (1967) in his landmark Privacy and Freedom, holds that individuals possess an inherent interest in controlling information about themselves. The second vision treats data protection primarily through a market-efficiency lens, viewing personal information as an economic good subject to contractual exchange and consumer choice. The tension between these perspectives informs virtually every contemporary regulatory debate.

Warren and Brandeis (1890) first articulated the concept of a 'right to be let alone' in American legal discourse, a formulation that influenced privacy theory for over a century. More recently, Solove (2006) proposed a taxonomy of privacy harms—including information collection, aggregation, insecurity, and intrusion—that maps well onto the specific risks posed by e-commerce platforms. Solove argued that privacy cannot be adequately understood through a single unifying theory; instead, context matters, and the law must respond with contextually sensitive rules. This insight has direct relevance for e-commerce, where the acceptable use of personal data depends heavily on the reasonable expectations of consumers at the time of collection.

Bygrave (2014) offers a comparative legal analysis of data protection law across multiple jurisdictions, identifying convergence around key principles (transparency, proportionality, and individual rights) while noting significant divergence in enforcement architecture and cultural attitudes toward privacy. His work underscores the difficulty of achieving genuine harmonization in an international digital marketplace—a problem that platforms operating across borders continue to navigate.

Taken together, these foundational scholars reveal a persistent tension that structures the entire field: a rights-based camp, represented by Westin and Solove, argues that data protection must be grounded in individual dignity and contextual integrity, resisting reduction to contractual exchange; while a market-based camp treats consumer consent and competitive incentives as the primary regulatory mechanisms. Bygrave's comparative work demonstrates that neither approach has proven fully adequate in isolation—effective frameworks tend to combine rights-protective floors with market-compatible flexibility. For e-commerce specifically, this synthesis matters: platforms operate simultaneously as commercial actors subject to market discipline and as custodians of personal information that carries constitutional weight. The regulatory analysis in subsequent sections evaluates Indonesia's UU PDP against this dual standard.

2.2. Regulatory Frameworks: From GDPR to UU PDP

The GDPR is widely regarded as the most influential data protection regulation in the world. Kuner et al. (2020) describe it as a 'regulation of global reach' that effectively exports European privacy norms to any entity that processes the personal data of EU residents, regardless of where that entity is established. For e-commerce platforms, this means that a Tokopedia seller accepting orders from an EU customer must, in principle, comply with GDPR requirements—a practical challenge that highlights the complexity of transnational data governance.

Comparatively, Indonesia's UU PDP has been described by scholars at Swiss German University (Yulianto, 2025) as a significant legislative advancement, largely modelled on the GDPR, that establishes personal data as a legal subject deserving of constitutional protection. The law distinguishes between general personal data (name, address, contact details) and specific (sensitive) personal data (biometric data, health information, financial records, and criminal history), imposing stricter requirements for the latter.

Data subjects are granted rights to access, correction, deletion, and withdrawal of consent—rights that, once the implementing regulations and the planned Personal Data Protection Agency (Lembaga PDP) are established, will carry meaningful legal force.

However, scholars such as Judijanto (2024) have noted the risks of a 'legislation without enforcement' scenario, where the mere existence of a law provides false assurance without producing behavioral change. They argue that Indonesia's institutional framework—specifically the absence of an independent data protection authority as of 2025—leaves the UU PDP without adequate teeth. This assessment is echoed by comparative studies that highlight the EU's experience: even the GDPR, with its substantial fines and dedicated supervisory authorities, took several years to produce consistent enforcement outcomes across member states.

2.3. Consumer Trust and the Economics of Data Protection

Research consistently demonstrates a close relationship between data protection and consumer trust. A study by Strzelecki and Rizun (2022) found that approximately 65% of consumers affected by a data breach reported that they would likely cease doing business with the affected company. More strikingly, up to 80% of consumers stated they would abandon an e-commerce platform if they did not feel confident their data was secure. These figures have direct implications for platform operators: inadequate data protection is not merely a legal risk but a commercial liability.

Kumari et al. (2014), writing in Advances in Consumer Research, demonstrated that perceived privacy risk and hedonic motivation interact in complex ways in e-commerce decision-making. Consumers who derive high enjoyment from the online shopping experience may discount perceived risks, while those with high privacy salience may abandon platforms even in the absence of a confirmed breach. This behavioral complexity suggests that legal compliance alone is insufficient—platforms must also proactively communicate their data governance practices to build and sustain trust.

The economic dimensions of data breaches reinforce this point. IBM (2024) reported that lost business costs encompassing customer turnover, reputational damage, and operational downtime represented the largest single component of breach costs, averaging USD 1.63 million per incident. The global average cost per compromised record was USD 173, rising to USD 429 in the healthcare sector. For e-commerce retailers specifically, the FBI's Internet Crime Complaint Center reported USD 16 billion in total cybercrime losses in 2024, a 33% increase from the previous year.

3. METHODOLOGY

This study employs a qualitative literature review methodology, consistent with approaches commonly used in legal and socio-legal scholarship. The qualitative literature review is appropriate for this research objective because it enables the systematic synthesis of existing legal texts, empirical studies, case reports, and expert commentary without requiring the collection of primary data. Rather than testing a quantitative hypothesis, this study seeks to construct an interpretive account of how personal data protection operates in e-commerce environments, drawing on a curated body of authoritative sources.

The research process involved four stages. First, a systematic search was conducted across academic databases, including Google Scholar, SSRN, and LexisNexis, using terms such as 'personal data protection AND e-commerce,' 'GDPR AND platform compliance,' 'UU PDP Indonesia,' and 'data breach AND consumer trust.' The initial search returned approximately 340 candidate sources. Inclusion criteria required that sources: (a) were published in peer-reviewed journals, authoritative legal commentaries, or reports from recognized international bodies; (b) were published between 2015 and 2025 (with foundational theoretical works before 2015 included selectively for conceptual grounding); and (c) directly addressed personal data protection in either a legal, regulatory, or empirical e-commerce context. Exclusion criteria eliminated sources that were non-English without available translation, lacked identifiable authorship, or originated from sources without editorial oversight. Following screening, 42 sources were retained for substantive analysis. To minimize selection bias, the author applied a multi-database approach, deliberately sought out sources critical of or divergent from the dominant GDPR

model, and ensured geographic diversity by including scholarship from the Indonesian, ASEAN, European, and global contexts.

Second, publications were screened for relevance and quality, prioritizing peer-reviewed journal articles, authoritative legal commentaries, and reports from recognized international organizations (IBM, OECD, World Bank) published between 2015 and 2025. Third, data from identified sources were coded thematically around three core themes: (1) legal frameworks, (2) empirical breach evidence, and (3) governance challenges. Fourth, findings were synthesized and critically interpreted in light of the research questions.

This study acknowledges limitations inherent in the qualitative literature review approach. The selection of sources, while guided by explicit criteria, involves an element of researcher judgment. Additionally, because data protection law evolves rapidly, particularly in jurisdictions like Indonesia, where implementing regulations are still pending, some findings may require updating as new regulatory developments occur. These limitations are mitigated by the explicit documentation of search parameters and the triangulation of findings across multiple source types.

4. RESULTS AND DISCUSSION

4.1. The Scale and Pattern of E-Commerce Data Breaches

The empirical record of data breaches in e-commerce is substantial and growing. The number of data compromises reported in the United States alone rose from 447 in 2012 to over 3,200 in 2023—a more than sevenfold increase in just over a decade. Globally, over 500 million records were exposed in breaches in 2021 alone (Kumari et al., 2014). These figures, while drawn from diverse sectors, reflect a trend that is particularly pronounced in consumer-facing digital commerce.

Table 1 below presents a chronological record of significant data breach incidents affecting e-commerce and related digital commerce platforms, with particular attention to incidents relevant to the Indonesian market and key global cases.

Table 1. Significant E-Commerce and Digital Platform Data Breach Incidents (2018–2024)

Year	Incident / Platform	Records Compromised	Data Type Exposed	Estimated Loss / Impact
2018	Tokopedia (partial breach)	~91 million	Email, password, phone	Reputational; legal inquiry
2019	Bukalapak	~13 million	Email, username, password	Data sold on the dark web
2020	Tokopedia (confirmed)	91 million	Full user credentials	Sold for ~USD 5,000
2021	BPJS Kesehatan (gov. e-service)	~279 million	NIK, name, salary, family data	National security concern
2022	PayPal / Cash App (global)	~8–35 million	Financial, PII	Class-action lawsuits
2023	MOVEit / multiple e-com vendors	94+ million (cumulative)	PII, credentials, and financial	USD 15 billion+ total damage
2024	Multiple Indonesian gov. portals	Undisclosed (large scale)	National ID, health records	Accelerated UU PDP enforcement

Sources: IBM Security (2024); Shopify/RH-ISAC (2024); tech.co breach database (2024); iclg.com Indonesia Data Protection Report (2025); UpGuard (2024); Varonis (2025).

The pattern that emerges from Table 1 is not random. E-commerce breaches tend to target high-value data categories, such as financial credentials, national identity numbers, and behavioral profiles, and they disproportionately affect platforms with large user bases and limited security investment relative to the scale of their data operations. The 2020 Tokopedia breach, in which 91 million user records were reportedly sold on the dark web for approximately USD 5,000, illustrates how cheaply consumer data can be monetized once security perimeters are breached.

What makes the e-commerce context distinctive is the layered nature of its data processing architecture. Platforms do not merely process data themselvesthey rely on extensive networks of third-party vendors, payment processors, logistics providers, and marketing analytics firms, each of which represents a potential vulnerability. According to Shopify's 2024 Retail Cybersecurity Report, 30% of all retail breaches in 2024 involved a third-party compromise, nearly double the rate from 2023. This 'supply chain' dimension of e-commerce data risk has important implications for regulatory design: rules that apply only to the platform operator may leave significant portions of the data lifecycle unregulated.

The structural causes of these patterns warrant deeper analytical attention. The near-doubling of third-party breach rates in a single year is not incidental; it reflects a systemic governance failure in how platform operators manage downstream data custodians. Contractual data processing agreements, where they exist, frequently lack audit rights or minimum security standards—leaving the platform legally exposed but operationally blind to vendor vulnerabilities. This is compounded by a market concentration dynamic: smaller e-commerce operators and MSMEs, which lack the bargaining power of platforms like Shopee or Tokopedia, must accept standard vendor contracts with limited ability to negotiate data protection terms. The governance failure is therefore structural rather than merely technical: it originates in power asymmetries across the supply chain that regulation targeting only primary data controllers cannot adequately address. The legislative response—including Article 51 of UU PDP, which imposes liability on joint controllers and processors—is a meaningful attempt to close this gap, but without enforcement infrastructure, such provisions risk remaining aspirational.

4.2. Legal Frameworks: Strengths and Gaps

The GDPR, now in its seventh year of full enforcement, has produced a growing body of enforcement decisions that clarify the obligations of e-commerce operators. Notably, major platforms, including Amazon (fined EUR 746 million by Luxembourg's data protection authority in 2021), Meta, and Google, have faced significant sanctions for violations related to consent mechanisms and behavioral advertising. These cases establish that the GDPR's requirements are enforceable against the largest and most powerful digital actors, a precedent that strengthens the hand of consumers and regulators alike.

Indonesia's UU PDP, by contrast, entered into full legal effect on 17 October 2024, but without the institutional infrastructure necessary for credible enforcement. As of early 2025, the implementing government regulation (RPP PDP) had not been finalized—it was in its fourth harmonization process—and the national Personal Data Protection Agency had not yet been established (ICLG, 2025). This gap between legal text and institutional reality creates a period of regulatory uncertainty that may be exploited by non-compliant actors, particularly smaller e-commerce operators and MSMEs that lack the resources for proactive compliance.

A 2024 study by Swiss German University involving 126 Indonesian MSMEs found that compliance awareness was low, with limited technical knowledge, inadequate training resources, and an absence of structured governance frameworks identified as the primary obstacles (Yulianto, 2025). Larger corporations in banking, telecommunications, and major e-commerce platforms had generally progressed further in aligning with GDPR-equivalent standards, often driven by international business partner requirements rather than domestic regulatory pressure alone.

4.3. Key Legal Obligations Under UU PDP for E-Commerce Operators

Under Law No. 27 of 2022, e-commerce operators processing personal data of Indonesian citizens bear specific obligations regardless of where the platform is established—a provision that mirrors the GDPR's extra-territorial scope. Key obligations include: (1) obtaining explicit, informed consent before data collection; (2) limiting data collection to the minimum necessary for stated purposes; (3) appointing a Data Protection Officer (DPO) for large-scale or sensitive data processing operations; (4) conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities; (5) notifying data subjects and relevant authorities within a specified timeframe in the event of a breach; and (6) ensuring that international data transfers are conducted in compliance with established safeguards.

The law grants data subjects seven enumerated rights: the right to know the purpose and legal basis of processing; the right to access their data; the right to correct inaccurate data; the right to delete or destroy data; the right to withdraw consent; the right to object to automated processing; and the right to file objections regarding data processing decisions that have legal consequences for them. Non-compliance can result in administrative sanctions, fines of up to 2% of annual revenue, bans on data processing activities, and criminal liability for willful violations. These sanctions, though not yet actively enforced, signal a significant escalation of legal risk for non-compliant operators.

4.4. Discussion

4.4.1. The Gap Between Enactment and Enforcement

The central challenge facing personal data protection in e-commerce—not only in Indonesia but across many emerging economies—is the implementation gap: the distance between the legal text of a statute and the behavioral change it is intended to produce. Judijanto (2024) have characterized this as a structural problem arising from insufficient institutional capacity, limited judicial familiarity with data protection concepts, and the absence of a dedicated enforcement body. The lesson from more mature jurisdictions is instructive: the GDPR, despite the strength of its provisions and the sophistication of the EU's legal culture, produced minimal enforcement activity in its first two years largely because supervisory authorities were still establishing procedures and processing a backlog of complaints.

For Indonesia, this suggests that the period between the enactment of UU PDP and the eventual establishment of Lembaga PDP is not merely a bureaucratic transition—it is a critical window during which legal culture must be cultivated, organizational practices reformed, and public awareness elevated. More fundamentally, the analysis reveals an institutional failure that is not merely procedural: the absence of Lembaga PDP reflects a political economy in which data protection has historically been treated as a second-order priority relative to economic liberalization and platform growth. Closing the implementation gap will therefore require not only technical institution-building but a deliberate reorientation of regulatory philosophy—one that treats data protection as a precondition for sustainable digital commerce rather than a constraint upon it.

4.4.2. Technological Complexity and Platform Accountability

A recurring theme in the literature is the difficulty of applying law developed for identifiable actors to a technological environment characterized by distributed processing, algorithmic decision-making, and opaque data supply chains. Solove (2006) argued that privacy law tends to lag behind technological change because legislators and courts cannot anticipate how new data practices will affect individual interests. This is nowhere more evident than in e-commerce, where behavioral profiling, real-time bidding for advertising inventory, and AI-driven personalization systems process personal data in ways that consumers neither perceive nor understand.

The concept of 'privacy by design,' first articulated by Cavoukian (2009) and later codified in Article 25 of the GDPR, offers a promising response to this challenge. Rather than treating privacy as a compliance obligation imposed after systems are built, privacy by design requires that data protection principles be embedded into the architecture of platforms from the outset. For e-commerce operators, this means designing consent mechanisms that are genuinely meaningful rather than perfunctory; building data minimization into recommendation algorithms; and ensuring that third-party integrations are subject to contractual data protection obligations. The extent to which UU PDP's implementing regulations will incorporate privacy by design principles remains to be seen, but scholarly commentary (Yulianto, 2025) suggests that alignment with GDPR-equivalent standards is both feasible and advisable.

4.4.3. Consumer Literacy and the Consent Paradox

No discussion of personal data protection in e-commerce would be complete without addressing the consent paradox: the irony that the legal mechanism most commonly used to legitimize data processing—individual consent—is also the mechanism most routinely undermined by the information asymmetry between platforms and users. Consumers are presented with lengthy, opaque privacy policies

that few read, and fewer still comprehend. Studies have estimated that reading the privacy policies of all services an average American uses annually would consume approximately 76 work days (McDonald & Cranor, 2008) a figure that has likely grown with the proliferation of digital platforms.

UU PDP's consent requirements, which mandate that consent be 'explicit and voluntary' and that data subjects receive specific information about the purpose, duration, and legal basis of processing, represent a meaningful step forward. However, without active enforcement and consumer education, these requirements risk becoming paper formalities. Scholars at Universitas Tarumanagara (FH Untar, 2025) have argued that genuine consumer empowerment requires not only legal rights but also digital literacy programs that enable individuals to exercise those rights in practice. This is a dimension of data protection policy that falls outside the conventional scope of legal scholarship but is essential to the social goals that data protection law is intended to serve.

4.4.4. Cross-Border Dimensions and International Harmonization

Indonesia's UU PDP, like the GDPR before it, adopts an extra-territorial scope that applies to any organization processing the personal data of Indonesian citizens, regardless of where that organization is established. This is a legally ambitious position that reflects the global nature of e-commerce but creates enforcement challenges when the data controller is located in a jurisdiction with different standards or limited diplomatic engagement with Indonesia.

As Cisometric (2025) has noted, Indonesia's recognition as a jurisdiction offering 'adequate' data protection by the EU—which would facilitate data transfers between the two regions—depends on factors including the establishment of Lembaga PDP, the finalization of implementing regulations, and demonstrated enforcement practice over time. The precedent set by the EU's Schrems I and II judgments, which invalidated the Safe Harbor and Privacy Shield arrangements with the United States because US surveillance law did not offer equivalent protection, illustrates the high standards that adequacy determinations impose. For Indonesian e-commerce operators seeking to engage European customers, or for European companies processing Indonesian consumer data, this regulatory uncertainty introduces tangible commercial risk.

5. CONCLUSION

Personal data protection in e-commerce platforms represents one of the defining legal challenges of the digital era. This article has demonstrated, through a qualitative review of legal texts, empirical data, and scholarly commentary, that the problem is multidimensional: it encompasses questions of institutional design, technology governance, consumer psychology, and international legal relations.

The enactment of Indonesia's UU PDP in 2022 represents a genuine legislative achievement that positions the country within the emerging community of states committed to comprehensive data protection. However, the article's findings underscore that legislation is a necessary but not sufficient condition for effective protection. The absence of an independent enforcement authority, incomplete implementing regulations, low compliance awareness among MSMEs, and the structural complexity of e-commerce data ecosystems all constitute significant obstacles that require sustained policy attention.

Several recommendations emerge from this analysis. First, the establishment of Indonesia's Lembaga PDP should be treated as a matter of urgency, with adequate resources and statutory independence to ensure credible enforcement. Second, implementing regulations should incorporate privacy by design requirements, mandating that e-commerce platforms embed data protection into their technical architecture rather than treating it as a compliance overlay. Third, the government and relevant civil society organizations should invest in digital literacy programs that enable consumers to exercise their rights under the UU PDP meaningfully. Fourth, Indonesia should pursue bilateral and multilateral data governance dialogues—including with ASEAN partners and the EU—to build toward mutual recognition frameworks that facilitate cross-border commerce while protecting consumer data. Fifth, sector-specific guidance for e-commerce operators, particularly MSMEs, should be developed to lower the compliance cost of legal adherence.

The stakes of this policy agenda are high. As the Advances in Consumer Research study (Kumari et al., 2014) demonstrated, up to 80% of consumers may abandon a platform they do not trust with their data. In a digital economy where consumer trust is the foundation of commercial viability, personal data protection is not merely a legal obligation—it is an economic imperative. Governments, platforms, and scholars who recognize this connection are better positioned to advance both the interests of consumers and the vitality of the digital economy that serves them.

Ethical Approval

This study was conducted in accordance with the ethical principles outlined in the Declaration of Helsinki. As a qualitative literature review relying solely on publicly available published sources, formal ethical committee approval was not required.

Informed Consent Statement

Not applicable. This study is based entirely on published literature and does not involve human participants.

Authors' Contributions

Not applicable

Disclosure Statement

No potential conflict of interest was reported by the author.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

This research received no external funding.

Notes on Contributors

Inggret Adu
Inggret Adu is a law student at the Faculty of Law, Social Sciences, and Political Science, Universitas Terbuka, Indonesia. Her research interests encompass digital law, personal data protection, and e-commerce regulation. This article represents her contribution to the growing body of Indonesian scholarship on the intersection of technology governance and consumer rights.

REFERENCES

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

Cisometric. (2025). *Comparing Indonesia's PDP law with GDPR and U.S. privacy rules*. https://www.cisometric.com/articles/comparing-indonesias-pdp-law-with-gdpr-and-us-privacy-rules

CMS Law. (2024). *Compliance with Indonesia's Personal Data Protection Law by October 2024*. https://cms.law/en/int/legal-updates/compliance-with-indonesias-personal-data-protection-law-by-october-2024

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union, L 119/1.

FBI Internet Crime Complaint Center. (2024). *2024 Internet crime report*. Federal Bureau of Investigation. https://www.ic3.gov

FH Untar. (2025). *Perlindungan data pribadi: Implementasi UU No. 27 Tahun 2022 dan tantangan penegakannya*. Universitas Tarumanagara Faculty of Law. https://fh.untar.ac.id

IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation. https://www.ibm.com/security/data-breach

International Comparative Legal Guides (ICLG). (2025). *Data protection laws and regulations: Indonesia 2025–2026*. https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights, 3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Kumari, M., Sinha, P. C., & Priya, S. (2014). The impact of data breaches on consumer trust in e-commerce. *International Journal of Current Science, 4*(4), 1–9. https://rjpn.org/IJCSPUB/papers/IJCSP14D1001.pdf

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 543–568. https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

Organisation for Economic Co-operation and Development. (2013). *The OECD privacy framework* (Updated ed.). OECD Publishing. https://doi.org/10.1787/9789264195387-en

Republic of Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law No. 11 of 2008 on Electronic Information and Transactions], as amended by Law No. 1 of 2024*.

Republic of Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection]*. State Gazette of the Republic of Indonesia, No. 196 of 2022.

Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) & Shopify. (2024). *Retail cybersecurity statistics 2024*. https://www.shopify.com/enterprise/blog/retail-cybersecurity

Yulianto, S. (2025). From policy to practice: How Indonesia's UU PDP 2022 shapes cybersecurity readiness in 2025. *Swiss German University Research Bulletin, 6*(1), 14–29. https://sgu.ac.id/uu-pdp-2022-indonesia-cybersecurity-readiness-2025/

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?params=/context/faculty_publications/article/2074/&path_info=A_Taxonomy_of_Privacy.pdf

Strzelecki, A., & Rizun, M. (2022). Trust erosion and consumer attrition following e-commerce data breaches: Behavioral evidence. *Electronic Commerce Research and Applications, 53*, Article 101145. https://doi.org/10.1016/j.elerap.2022.101145

Varonis Systems. (2025). *2025 data breach statistics and trends*. https://www.varonis.com/blog/data-breach-statistics

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.