Analysis of Legal Protection for Tokopedia Consumer Data in Data Leakage Cases in Indonesia

La Sirajuddin[1], Dwi Pratiwi Markus[2]

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

*correspondence email: lasirajuddin853@gmail.com

Abstract: The aim of this study is to examine the strength of legal protection for Tokopedia customers' personal data following the leak of 91 million accounts in May 2020, as well as to explain Tokopedia's obligations and responsibilities as a data controller under PDP Law 27/2022, UUPK 8/1999, ITE Law 11/2008, PP 71/2019, and the breach of contract provisions of Article 1234 of the Civil Code. **This study uses** a normative legal approach, which involves examining written regulations through laws, scientific journals, and official reports from the Ministry of Communication and Information Technology, then analyzing them conceptually and comparing them to assess legal certainty, fairness, and benefits for the community. **The novelty** of this research lies in combining classical civil law (breach of contract in the Civil Code) with new regulations in the PDP Law to assess Tokopedia's responsibility as a private PSE in the case of the leak of 91 million accounts, something that is still rarely discussed comprehensively in Indonesian literature. **The results** of the study show that the rules on personal data protection are actually quite strong on paper, but their implementation is still weak because Tokopedia has not maximized its assessment of data protection, encryption, and incident reporting; the public's level of understanding of their personal data rights is still low; and the government's response has only been in the form of warnings, so there is still the possibility of administrative sanctions, fines, or criminal penalties being imposed based on the PDP Law and the ITE Law. **The conclusion** of the study emphasizes the need to strengthen personal data protection through mandatory information security standards such as ISO 27001, the application of the principle of privacy by design from the outset of system design, the provision of features (dashboards) for rapid data deletion, increased public education, and better coordination between Kominfo, OJK, and the PDP Council so that e-commerce transactions in Indonesia are safer for hundreds of millions of users.

Keywords: Personal Data; E-Commerce; Consumer Protection; Data Breachs; Breach of Contract.

Abstrak: Tujuan penelitian adalah melihat seberapa kuat perlindungan hukum atas data pribadi pelanggan Tokopedia setelah kebocoran 91 juta akun pada Mei 2020, serta menjelaskan kewajiban dan tanggung jawab Tokopedia sebagai pengendali data menurut UU PDP 27/2022, UUPK 8/1999, UU ITE 11/2008, PP 71/2019, dan aturan wanprestasi Pasal 1234 KUHPerdata. Metode penelitian menggunakan pendekatan hukum normatif, yaitu meneliti aturan tertulis melalui undang-undang, jurnal ilmiah, dan laporan resmi Kominfo, kemudian dianalisis secara konseptual dan dibandingkan untuk menilai kepastian hukum, keadilan, dan

kemanfaatan bagi masyarakat. **Kebaruan penelitian** *terletak pada penggabungan hukum perdata klasik (wanprestasi KUHPerdata) dengan aturan baru dalam UU PDP untuk menilai tanggung jawab Tokopedia sebagai PSE privat dalam kasus kebocoran 91 juta akun, sesuatu yang masih jarang dibahas secara utuh di literatur Indonesia.* **Hasil penelitian** *menunjukkan bahwa aturan tentang perlindungan data pribadi sebenarnya sudah cukup kuat di atas kertas, tetapi penerapannya masih lemah karena Tokopedia belum maksimal melakukan penilaian dampak perlindungan data, enkripsi, dan pelaporan insiden; tingkat pemahaman masyarakat tentang hak data pribadinya masih rendah; dan respons pemerintah hanya berupa teguran sehingga masih ada peluang dijatuhkannya sanksi administratif, denda, maupun pidana berdasarkan UU PDP dan UU ITE.* **Kesimpulan penelitian** *menekankan perlunya penguatan perlindungan data pribadi melalui kewajiban standar keamanan informasi seperti ISO 27001, penerapan prinsip privacy by design sejak awal sistem dirancang, penyediaan fitur (dashboard) untuk penghapusan data secara cepat, peningkatan edukasi kepada masyarakat, serta koordinasi yang lebih baik antara Kominfo, OJK, dan Dewan PDP agar transaksi e-commerce di Indonesia lebih aman bagi ratusan juta pengguna.*
Kata Kunci: *Data Pribadi; E-Commerce; Perlindungan Konsumen; Kebocoran Data; Wanprestasi.*

1. INTRODUCTION

Indonesia, as a country based on law in accordance with Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, guarantees comprehensive protection of human rights, including the privacy of personal data in digital transactions that increasingly dominate everyday life. Article 28G paragraph (1) of the 1945 Constitution explicitly states that every person has the right to protection of their personal life, family, honor, dignity, and the right to security and protection from fear of acting or not acting as a human right, thus becoming the constitutional basis for strengthening data protection regulations in the information age.[1]

The rapid development of information and communication technology has brought fundamental changes to various aspects of human life, especially in social interaction, economic activity, and electronic commerce. Wider internet access, advanced cloud computing infrastructure, and sophisticated mobile applications have made it easier for people to access information instantly, communicate across national borders, and conduct sales transactions through e-commerce platforms with a high level of convenience.[2]

In Indonesia, the e-commerce sector has grown exponentially since the COVID-19 pandemic, not only supporting the national economy through significant contributions to GDP, but also empowering millions of Micro, Small, and Medium Enterprises (MSMEs) through supply chain digitalization, online marketing, and integrated logistics distribution. Tokopedia, founded in 2009 as a local marketplace, has grown into one of the dominant platforms with a

---

[1] Muhammad Ridwan Arifin dan R. Ahmad Syahroni, "Urgency of Private Data Protection in the Digital Communication Era," *International Journal of Global Community* 1, no. 2 (2018): 123–140.

[2] Supriadin dan Wardan, "Dampak Kemajuan Teknologi Informasi dalam Transformasi Bisnis dan Ekonomi di Indonesia," *Economica Insight* 2, no. 1 (2025): 21–30.

user base reaching hundreds of millions, offering innovative features such as Tokopedia Play for entertainment, digital top-ups, and integration with Gojek after the merger into GoTo, which further expands its digital ecosystem.[3]

However, this progress comes with critical risks related to consumer data security and privacy protection, where personal data has become a highly valuable asset that includes information on consumer identity, finances, and behavior. The Tokopedia data breach incident in March-April 2020 became a landmark case that shook the Indonesian e-commerce industry: a hacker named "gnosticplayers" managed to steal 91 million user data records, including full names, email addresses, phone numbers, dates of birth, gender, and MD5 password hashes that were vulnerable to hacking, before selling them on a dark web forum for around 5,000 USDT and sharing them for free on Facebook.[4] The impacts were far-reaching, ranging from mass phishing threats and identity theft to financial losses for Tokopedia due to a temporary decline in user traffic and significant forensic investigation costs, while also shaking public confidence in the security of digital transactions as a whole.

Although the legal framework has been strengthened through Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which regulates the obligations of data controllers and processors regarding the principles of transparency, accountability, security, and data subject rights such as informed consent, the right to be forgotten, and data portability, its implementation on platforms such as Tokopedia still faces significant challenges. Violations in 2020 occurred before the PDP Law came into full effect (October 2024), but it revealed loopholes in previous regulations such as Government Regulation No. 71 of 2019 concerning Electronic System and Transaction Organization and Minister of Communication and Information Technology Regulation No. 20 of 2016 concerning Personal Data Protection in the Electronic Sector, where the absence of independent audits, strong encryption, and a Computer Security Incident Response Team (CSIRT) were contributing factors.[5]

Previous studies have provided valuable insights but remain fragmented. A study titled "Legal Analysis of Privacy Policies and Online Marketplace Legal Responsibility in Protecting User Personal Data in Data Breach Cases" by Maichle Delpiero et al. (2021) analyzed the privacy policies of platforms such as Tokopedia, Bukalapak, and Bhinneka, finding inconsistencies with regulations prior to the Personal Data Protection (PDP) Law and weaknesses in legal liability, thus recommending stronger regulations and strict enforcement.[6]

---

[3] Inas Nurfadia Futri, Fifi Afisah, dan Muhammad Sholahuddin, "Tokopedia's Strategy in Helping Indonesia's Economic Recovery during the Covid-19 Pandemic through the Digitalization of MSMEs," *Sebelas Maret Business Review* 6, no. 1 (2021): 1–15

[4] Afip et al., "Analisis Insiden Kebocoran Data 91 Juta Akun Tokopedia: Dampak dan Upaya Penanganannya," *Integrative Perspectives of Social and Science Journal* 2, no. 3 (2025): 4858–65

[5] I Wayan Cenik Ardika, "Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce," *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 1–11.

[6] Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, dan Nafisah Muthmainnah, "Legal Analysis of

Meanwhile, "Analysis of Data Privacy Violations on the Tokopedia E-Commerce Platform" by Sinta Sukma Ayu and Muhammad Irwan Padli Nasution (2023) uses a qualitative literature review method to analyze a data breach of 91 million records, highlighting the platform's weak security system and non-compliance with PP 71/2019 and Permenkominfo 20/2019, as well as emphasizing the need for regulatory reform to minimize risks. More recently, "The Implications of the Personal Data Protection Law for Consumers in E-Commerce Transactions" by Muhammad Rasid (2025) conducted a normative legal analysis, concluding that the PDP Law requires platforms to be responsible for data processing with criminal and administrative sanctions (up to 10 years in prison and a maximum fine of IDR 100 million). - Commerce" by Muhammad Rasid (2025) conducted a normative juridical analysis, concluding that the PDP Law requires platforms to be responsible for data processing with criminal, administrative (up to 2% of global turnover), and civil sanctions, and calls for improved compliance and oversight mechanisms.[7]

However, the most notable research gap is the lack of comprehensive studies that integrate Tokopedia's case analysis with the legal framework following the Personal Data Protection (PDP) Law, particularly in evaluating the effectiveness of implementations such as Data Protection Impact Assessments (DPIAs), cross-border data transfers, and coordination between authorities (PDP Authority with OJK and KPPU). This gap is exacerbated by the absence of technology-based practical recommendations such as zero-trust architecture and AI-based threat detection, as well as long-term economic impact analysis on MSMEs that depend on the platform.[8]

The novelty of this research lies in its holistic interdisciplinary approach: analyzing the Tokopedia case as a systemic representation, within the context of the PDP Law and its derivatives, to fill this gap through specific and actionable legal accountability mapping. The research objectives are: (1) To determine Tokopedia's legal accountability in protecting consumer personal data during transactions according to applicable regulations in Indonesia; (2) To determine Tokopedia's responsibility for consumer personal data breaches, including legally mandated prevention and recovery measures.

2. METHOD

This study employs a normative juridical approach using secondary data consisting of primary, secondary, and tertiary legal materials. The primary legal materials include Law No. 27 of 2022 on Personal Data Protection, Law No. 8 of 1999 on Consumer Protection, Law No.

Online Marketplace Privacy Policy and Accountability in Protection of Users' Personal Data on Data Leakage Cases," *Padjadjaran Law Review* 9, no. 1 (2021): 1–23.

[7] Sinta Sukma Ayu dan Muhammad Irwan Padli Nasution, "Analysis of Data Privacy Breach on Tokopedia E-Commerce," *Jurnal Hukum E-Commerce* 5, no. 2 (2023): 120–145.

[8] Alif Rinoko Fajar, "Analisis Kebijakan Undang-Undang Perlindungan Data Pribadi Sebagai Pemenuhan Hak Asasi Manusia: Studi Kasus Tokopedia," *Jipolis: Jurnal Ilmu Politik dan Ilmu Sosial* 1, no. 3 (2024): 1–15

11 of 2008 on Electronic Information and Transactions as amended by Law No. 1 of 2024, the Indonesian Civil Code, and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions.

Secondary legal materials include scholarly journals, legal textbooks, scientific articles, academic research findings, and opinions of legal experts related to personal data protection, the liability of e-commerce providers, and law enforcement mechanisms. Tertiary legal materials, such as legal dictionaries and legal encyclopedias, are used to clarify technical terms.

The data collection technique is carried out through normative juridical research, namely a literature study that involves searching for, reading, and carefully reviewing various relevant legal sources. The collected data are then analyzed qualitatively by using a statute approach to examine the applicable normative provisions and a conceptual approach to analyze the legal theories and doctrines underlying the legal protection of consumer data in e-commerce. This study also employs a case approach to the 2020 Tokopedia data breach incident as an illustration of the application of legal norms in practice. This research is prescriptive in nature, aiming to formulate recommendations for strengthening the legal protection of personal data.

3. DISCUSSION

3.1. Legal Responsibility for the Protection of Consumers' Personal Data on the Tokopedia Platform.

Legal responsibility for the protection of consumers' personal data on the Tokopedia platform stems primarily from Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law binds Tokopedia as the data controller to secure consumer information like names, addresses, emails, phone numbers, birth dates, and financial data during e-commerce transactions. These details are vulnerable to misuse, identity theft, phishing, or illegal sales if leaked, as in the 2020 breach of 91 million records. The PDP Law requires explicit consent before collection, regular security audits, privacy-by-design, and a Data Protection Officer. It also mandates breach reporting to authorities within 72 hours to limit harm.[9]

Article 16 of the PDP Law outlines key principles: purpose limitation, processing limits, data minimization, accuracy, integrity, and security. Tokopedia must process data transparently, proportionately, and only for valid purposes while blocking unlawful access or changes. As controller, Tokopedia faces administrative sanctions like fines up to 2% annual revenue for non-compliance. Criminal penalties apply for intentional breaches causing harm to consumers. This framework ensures accountability beyond mere compliance.[10]

---

9 Ragil Putri Anindya dan Achmad Edi Subiyanto, "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi," *Journal of Artificial Intelligence and Digital Business (RIGGS)* 4, no. 3 (2025): 1105–1112.

10 Muhammad Iqbal dan Tim Penulis, "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi," *Jurnal Innovative: Journal of Social Science Research* 6, no. 2 (2025): 13476–13490.

From civil law, the user-Tokopedia tie is contractual via Terms of Service and Privacy Policy acceptance. Tokopedia promises a secure system under UU ITE and PP 71/2019 on data protection implementation. The 2020 leak of 91 million profiles beyond 65.65 million active accounts shows clear contract breach. Inadequate safeguards like weak hashing exposed user details to dark web sales. This violated promised reliability in electronic transactions. This qualifies as wanprestasi under KUHPerdata Articles 1234, 1238, and 1243 due to poor encryption and delayed detection. Consumers can claim material damages (fraud losses), immaterial harm (distress), costs, and interest. Law No. 8/1999 on Consumer Protection (Articles 4, 19) bolsters this, ensuring safety from business negligence. It mandates comfort and security in digital services. Victims gain stronger grounds for compensation claims.

In practice, the 2020 KKI class action against Tokopedia and Kominfo at Jakarta Court sought license revocation and Rp100 billion fines. It was dismissed on absolute incompetence grounds, shifting to TUN jurisdiction without substantive review. Procedural barriers blocked examination of wanprestasi and PDP violations. This reveals enforcement gaps despite strong norms. Judicial efficiency suffers in data disputes. Pre-PDP rules like UU ITE offered general protection without firm breach accountability.[11] Post-2022 PDP demands end-to-end encryption and 3x24-hour notifications. Recommendations include BSSN-standardized security protocols nationwide. OJK/BPKN mediation can bypass court hurdles effectively. Consumer literacy programs build awareness of rights.

This normative analysis confirms Tokopedia's full liability as controller, with wanprestasi enabling claims. Procedural reforms like special data courts are vital for redress. Tokopedia should adopt GDPR-aligned tools proactively. Policymakers must enact derivative regulations swiftly. Effective enforcement restores e-commerce trust in Indonesia.

Based on normative analysis, this research finds that (1) Tokopedia bears full responsibility as data controller for the 2020 breach under PP 71/2019 and PDP Law, including administrative sanctions and KUHPerdata wanprestasi compensation; (2) Internal policies and technical measures require total audits with ISO 27001, DPIA, DPO to comply with Article 16 PDP Law principles; (3) Dispute mechanisms, 72-hour notifications, user literacy, and BSSN cooperation are essential to prevent enforcement barriers like court jurisdiction issues.

3.2. Tokopedia's Responsibility for Personal Data Breaches and Strengthening Measures.

As an electronic system provider and personal data controller, Tokopedia bears significant legal responsibility for personal data breaches. The May 2020 breach involved 91 million user records hacked and sold on the dark web. This demonstrates suboptimal fulfillment of data controller protection duties, causing serious losses and risks for millions of

---

[11] Dipo Abdila Rasyid, "Analisis Legal Standing Komunitas Konsumen Indonesia Selaku Lembaga Perlindungan Konsumen Swadaya Masyarakat dalam Permasalahan Perlindungan Data Pribadi Konsumen Pengguna E-Commerce Tokopedia (Studi Kasus Putusan Nomor 235/Pdt.G/2020/PN.Jkt.Pst)" (Skripsi S1, Universitas Indonesia, 2023).

users. Pre-PDP Law 2022, liability stemmed from PP 71/2019 on PSE requiring confidentiality, integrity, and data availability. Tokopedia is deemed to violate obligations, exposed to administrative, civil, and criminal sanctions.

Post-PDP Law 2022, Tokopedia's accountability standards become more explicit and detailed. Data controllers must conduct Data Protection Impact Assessment (DPIA) for high-risk processes. Prevent unlawful processing, block illegal access, notify data owners promptly. Demonstrate application of accountability, minimization, and data security principles. With massive data volume, permanent Data Protection Officer (DPO) appointment is mandatory.[12]

Comprehensive steps to enhance Tokopedia data protection are urgently needed. Begin with thorough audits aligning all internal policies with PDP Law. Review service contracts, privacy documents, and daily technical operations. Reform standard terms to comply with regulations and protect user rights. Make audits the foundation for sustainable system transformation.[13] Next, strengthen information security infrastructure with layered protocols. Adopt ISO/IEC 27001 as information risk management standard. Implement full encryption for critical data, strict dual authentication (MFA). Conduct regular penetration testing and vulnerability scanning. Install 24/7 threat detection sensors.[14]

Then apply integrated privacy concepts from product design stage. All innovative features must pass pre-release DPIA. Set privacy-friendly default settings, disable automatic data sharing. This approach anticipates risks from system roots. Fully compliant with Article 16 PDP Law mandate. Subsequently, simplify and clarify privacy policy with tiered format. Use plain language with essential summary upfront. Explain data types, collection purposes, recipients, consumer rights. Make consent genuinely informative, not mere checkboxes. Maximize clarity for all users.[15]

Further, establish fast channels fulfilling data subject rights. Facilitate access, correction, deletion, processing restriction. Provide intuitive app portals with transparent procedures. Document every request for audit evidence. Empower consumers within platform ecosystem.

Complete with dedicated data protection unit and official DPO appointment. Develop internal guidelines, monitor daily compliance, train relevant staff. Maintain smooth communication with regulators and data owners. Position this function as long-term corporate strategy pillar. Treat PDP as cross-divisional priority beyond IT concerns.[16]

Equally important, perfect incident response protocols and 72-hour breach reporting.

---

[12] Muhammad Arifin Rinjani, "Hambatan Implementasi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Strategi Penguatan Pengawasannya," *Jurnal Administratum* 13, no. 1 (2025): 45–60

[13] Gomulia, O., et al., "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022," *Journal of World Science* 3, no. 4 (2024): 4234–4243.

[14] Unit Kompetensi, "Keamanan E-Commerce dengan ISO 27001: Standar Wajib untuk Perlindungan Data," *Blog Unit Kompetensi*, May 7, 2025

[15] Putri E. Sembiring, "Implementasi Desain Privasi sebagai Bentuk Perlindungan Data Pribadi Pengguna Aplikasi PeduliLindungi," *Veritas: Jurnal Teknik Hukum dan Masalah-Masalah Hukum* 20, no. 1 (2024): 1–20

[16] Benny Martha Dinata, "Implementasi Hak Subjek Data dalam Undang-Undang Pelindungan Data Pribadi: Tantangan dan Efektivitas," *Quantum Juris: Jurnal Hukum Modern* 8, no. 1 (Januari 2026): 446–53

Create clear workflow for identification, root analysis, impact classification, communication. Instant remediation actions reduce damage escalation. Seamless coordination with BSSN and OJK. Implement valuable lessons from 2020 incident.[17] Further, build close synergy with government oversight agencies. Support routine inspections, follow BSSN directives, report transparently. Demonstrate genuine commitment to PDP regulatory compliance. Facilitate effective supervision for consumer guarantees. Prioritize operational transparency and accountability.[18]

Additionally, design user-friendly dispute resolution and compensation pathways. Offer fast mediation and hassle-free digital claims with low costs. Establish fair compensation scheme proportional to actual damages. Avoid lengthy litigation traps like previous KKI case. Concretely restore public trust.[19] Finally, launch massive education campaigns on data protection awareness. Provide practical guides within app about account security. Send regular reminders on safe practices, smart phishing avoidance. Activate users as frontline self-protection guards. Legal literacy collaboration enhances system effectiveness.[20]

Based on normative analysis, this research finds that (1) Tokopedia bears full responsibility as data controller for 2020 breach under PP 71/2019 and PDP Law, including administrative sanctions and KUHPerdata wanprestasi compensation; (2) Internal policies and technical measures require total audits with ISO 27001, DPIA, DPO to comply with Article 16 PDP Law principles; (3) Dispute mechanisms, 72-hour notifications, user literacy, and BSSN cooperation are essential to prevent enforcement barriers like court jurisdiction issues.

4. CONCLUSION

This study reveals that legal protection of consumer personal data on Tokopedia is based on three main pillars: the Personal Data Protection Act (PDP) of 2022, the Consumer Protection Act of 1999, and the Electronic Information Act of 2008. The implementation of this protection is still weak due to platform security gaps, suboptimal enforcement of supervision, and low consumer awareness. As a data controller, Tokopedia is fully responsible for violations based on the principles of civil contracts (breach of contract) and PDP/Consumer laws, including data security obligations, user transparency, and compensation for losses. This study concludes that effective digital data protection requires holistic integration between normative, technical, and educational efforts through collaborative commitments between platforms, regulators, policymakers, and increasingly aware consumers to build a safe and

---

[17] Gerbang Pelindungan Data Pribadi Indonesia, "Data Protection By Design and By Default," June 8, 2024, https://gerbangpelindungandatapribadi.id/ensiklopedia-pdp/data-protection-by-design-and-by-default.

[18] Muhammad Gilang, "Pengawasan dan Penegakan Hukum E-Commerce oleh KPPU dalam Mengatasi Persaingan Usaha Tidak Sehat," *Rewang Rencang: Jurnal Hukum Lex Generalis* 5, no. 4 (2024): 275–290.

[19] Hukumonline, "Tanggung Jawab E-Commerce atas Kebocoran Data Pribadi," *Klinik Hukumonline*, November 2, 2022, https://www.hukumonline.com/klinik/a/tanggung-jawab-ie-commerce-i-atas-kebocoran-data-pribadi-lt63638331d18f0.

[20] A. Fadli Sutarli, Shelly Kurniawan, dan Tim, "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Sosialisasi Literasi Digital," *Jurnal Pengabdian Literasi Digital Indonesia* 2, no. 1 (2024): 1–1

sustainable e-commerce ecosystem in Indonesia.

REFERENCE

Afip et al., "Analisis Insiden Kebocoran Data 91 Juta Akun Tokopedia: Dampak dan Upaya Penanganannya," *Integrative Perspectives of Social and Science Journal* 2, no. 3 (2025): 4858–65, https://ipssj.com/index.php/ojs/article/view/578.

Alif Rinoko Fajar, "Analisis Kebijakan Undang-Undang Perlindungan Data Pribadi Sebagai Pemenuhan Hak Asasi Manusia: Studi Kasus Tokopedia," *Jipolis: Jurnal Ilmu Politik dan Ilmu Sosial* 1, no. 3 (2024): 1–15, https://ejournal.fisip.unjani.ac.id/index.php/jipolis/article/view/2543.

Dipo Abdila Rasyid. "Analisis Legal Standing Komunitas Konsumen Indonesia Selaku Lembaga Perlindungan Konsumen Swadaya Masyarakat dalam Permasalahan Perlindungan Data Pribadi Konsumen Pengguna E-Commerce Tokopedia (Studi Kasus Putusan Nomor 235/Pdt.G/2020/PN.Jkt.Pst)." Skripsi S1, Universitas Indonesia, 2023. https://lib.ui.ac.id/abstrakpdf?id=20518191&lokasi=lokal.

Fadli Sutarli, Shelly Kurniawan, dan Tim. "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Sosialisasi Literasi Digital." *Jurnal Pengabdian Literasi Digital Indonesia* 2, no. 1 (2024): 1–11. https://jurnal.relawantik.or.id/abdimas/article/view/122.

Gerbang Pelindungan Data Pribadi Indonesia. "Data Protection By Design and By Default." June 8, 2024. https://gerbangpelindungandatapribadi.id/ensiklopedia-pdp/data-protection-by-design-and-by-default.

Gomulia, O., et al. "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022." *Journal of World Science* 3, no. 4 (2022): 4234–4243. https://jws.rivierapublishing.id/index.php/jws/article/view/584.

Hukumonline. "Tanggung Jawab E-Commerce atas Kebocoran Data Pribadi." *Klinik Hukumonline*, November 2, 2022. https://www.hukumonline.com/klinik/a/tanggung-jawab-ie-commerce-i-atas-kebocoran-data-pribadi-lt63638331d18f0.

I Wayan Cenik Ardika. "Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce." *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 1–11. https://journal.pubmedia.id/index.php/lawjustice/article/view/3601.

Inas Nurfadia Futri, Fifi Afisah, dan Muhammad Sholahuddin. "Tokopedia's Strategy in Helping Indonesia's Economic Recovery during the Covid-19 Pandemic through the Digitalization of MSMEs." *Sebelas Maret Business Review* 6, no. 1 (2021): 1–15. https://jurnal.uns.ac.id/SMBR/article/download/55644/33864.

Kitab Undang-Undang Hukum Perdata (KUHPerdata). Pasal 1234, 1238, 1243.

Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, dan Nafisah Muthmainnah. "Legal Analysis of Online Marketplace Privacy Policy and

Accountability in Protection of Users' Personal Data on Data Leakage Cases." *Padjadjaran Law Review* 9, no. 1 (2021): 1–23. https://doi.org/10.23920/plr.v9i1.509.

Muhammad Arifin Rinjani. "Hambatan Implementasi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Strategi Penguatan Pengawasannya." *Jurnal Administratum* 13, no. 1 (2025): 45–60. https://journal.undiknas.ac.id/index.php/JAH/article/view/6793.

Muhammad Gilang. "Pengawasan dan Penegakan Hukum E-Commerce oleh KPPU dalam Mengatasi Persaingan Usaha Tidak Sehat." *Rewang Rencang: Jurnal Hukum Lex Generalis* 5, no. 4 (2024): 275–290. https://ojs.rewangrencang.com/index.php/JHLG/article/download/604/275/2192.

Muhammad Iqbal dan Tim Penulis. "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi." *Jurnal Innovative: Journal of Social Science Research* 6, no. 2 (2025): 13476–13490. https://j-innovative.org/index.php/Innovative/article/view/13476.

Muhammad Ridwan Arifin dan R. Ahmad Syahroni. "Urgency of Private Data Protection in the Digital Communication Era." *International Journal of Global Community* 1, no. 2 (2018): 123–140. https://journal.riksawan.com/index.php/IJGC-RI/article/view/49.

Benny Martha Dinata, "Implementasi Hak Subjek Data dalam Undang-Undang Pelindungan Data Pribadi: Tantangan dan Efektivitas," *Quantum Juris: Jurnal Hukum Modern* 8, no. 1 (Januari 2026): 446–53, https://journalversa.com/s/index.php/jhm/article/view/5080.

Putri E. Sembiring. "Implementasi Desain Privasi sebagai Bentuk Perlindungan Data Pribadi Pengguna Aplikasi PeduliLindungi." *Veritas: Jurnal Teknik Hukum dan Masalah-Masalah Hukum* 20, no. 1 (2024): 1–20. https://doi.org/10.28999/veritas.v10i1.7622.

Ragil Putri Anindya dan Achmad Edi Subiyanto. "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi." *Journal of Artificial Intelligence and Digital Business (RIGGS)* 4, no. 3 (2025): 1105–1112. http://journal.ilmudata.co.id/index.php/RIGGS/article/view/2105.