

LEGAL PROTECTION OF MARKETPLACE USERS' PERSONAL DATA FROM THE PERSPECTIVE OF THE PERSONAL DATA PROTECTION LAW

Robinson Bhayangkara¹
Universitas Mahendradatta

Erikson Sihotang²
Universitas Mahendradatta

Komang Edy Dharma Saputra³
Universitas Mahendradatta

Correspondence : Robinson Bhayangkara (Robinsonbhayangkara@gmail.com)

ABSTRACT

The rapid growth of online marketplaces in Indonesia has made the collection and processing of consumers' personal data an integral part of everyday commerce, encompassing identity information, payment and financial details, delivery addresses, transaction history, and behavioural data used for targeted advertising. This large-scale accumulation of personal data by marketplace platforms creates significant exposure to misuse, unauthorised disclosure, and security breaches, as illustrated by well documented incidents affecting major Indonesian e-commerce platforms. This article examines the legal protection afforded to marketplace users' personal data under Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), Indonesia's first comprehensive, cross-sectoral data protection statute. Using a normative juridical method with statutory, conceptual, and case-based approaches, this study analyses how the UU PDP's data subject rights, controller and processor obligations, breach notification requirements, and administrative and criminal sanctions apply to the marketplace context, and evaluates these protections against the classical Indonesian legal-protection theory distinguishing preventive from repressive protection. The study finds that the UU PDP substantially strengthens the legal position of marketplace users by, for the first time, imposing an explicit, time-bound breach notification duty, requiring a documented lawful basis and, in most cases, explicit consent for processing, and creating both administrative sanctions enforceable by a dedicated supervisory authority and criminal penalties for unlawful collection, disclosure, use, or falsification of personal data. At the same time, the study identifies persisting gaps in practical protection, including the continuing prevalence of take-it-or-leave-it consent mechanisms embedded in marketplace terms of service, extensive and often opaque data sharing with third-party logistics, payment, and advertising partners, unresolved questions concerning cross-border transfer of user data to overseas cloud infrastructure, and the still-developing institutional capacity of Indonesia's Personal Data Protection Supervisory Authority. The article concludes that effective protection of marketplace users' personal data requires not only continued reliance on the UU PDP's civil, administrative, and criminal mechanisms but also sector-specific implementing regulation for electronic commerce and strengthened institutional enforcement capacity.

Keywords: personal data protection; marketplace; e-commerce; data subject rights; Personal Data Protection Law

INTRODUCTION

The expansion of online marketplaces has fundamentally transformed the structure of retail commerce in Indonesia, with national e-commerce transaction value growing from

approximately one hundred six trillion rupiah in 2018 to more than two hundred sixty-six trillion rupiah in 2020 alone, a trend accelerated by the operational necessities of the COVID-19 pandemic and sustained thereafter by continuing consumer adoption of digital shopping. Every transaction conducted through a marketplace platform, whether a purchase of goods, a payment through an integrated digital wallet, or the simple act of registering a user account, necessarily involves the collection and processing of personal data, ranging from basic identity information such as name, telephone number, and email address, to more sensitive categories such as payment card details, bank account numbers, precise delivery addresses, and behavioural data derived from browsing and purchase history that platforms routinely use to power personalised recommendations and targeted advertising.

This large-scale accumulation of personal data within a small number of dominant marketplace platforms creates a correspondingly large attack surface for data misuse and unauthorised disclosure, and Indonesia's recent history offers concrete illustration of the resulting risk. In March 2019, the marketplace Bukalapak experienced a security breach reportedly affecting approximately thirteen million customer records, and in May 2020 the marketplace Tokopedia experienced a considerably larger breach in which data associated with approximately ninety-one million customer accounts and seven million seller accounts was reportedly offered for sale on a dark web forum. The Tokopedia breach subsequently led the Indonesian Consumers Community (Komunitas Konsumen Indonesia) to file a civil lawsuit against Tokopedia and the Minister of Communication and Information Technology before the Central Jakarta District Court, registered under case number 235/PDT.G/2020/PN.JKT.PST, illustrating both the tangible consumer harm that can follow from platform-level data breaches and the historically limited and fragmented legal avenues available to affected users prior to the enactment of a comprehensive data protection statute.

At the time of the Bukalapak and Tokopedia incidents, Indonesia lacked a single, comprehensive statute governing the processing of personal data across sectors, relying instead on a patchwork of sector-specific and comparatively general provisions, including the Electronic Information and Transactions Law and its implementing regulations, most notably Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and the earlier Ministerial Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, none of which established a dedicated independent supervisory authority, a codified set of data subject rights comparable to international standards, or a clear, time-bound breach notification obligation. This regulatory gap was substantially addressed by the enactment of Law Number 27 of 2022 concerning

Personal Data Protection (UU PDP) on 17 October 2022, which for the first time establishes a comprehensive, cross-sectoral framework governing the processing of personal data by both public and private entities, including marketplace platforms acting as personal data controllers.

Against this background, this article examines how the legal protection of marketplace users' personal data is structured under the UU PDP, and evaluates the extent to which this new statutory framework closes the protective gaps exposed by prior incidents such as the Bukalapak and Tokopedia breaches. The discussion addresses two research questions: first, how the UU PDP allocates rights to marketplace users as data subjects and corresponding obligations to marketplace platforms as data controllers and, where applicable, data processors; and second, what preventive and repressive legal protection mechanisms the UU PDP makes available to marketplace users, and what practical and institutional obstacles continue to limit the effectiveness of that protection. The scope of this study is confined to the personal data protection dimension of marketplace transactions and does not extend to the separate questions of product liability, payment system regulation, or platform antitrust concerns, except where directly relevant to contextualise the data protection analysis.

RESEARCH METHOD

This study employs a normative juridical method, appropriate to a research problem concerned with the interpretation and systematic mapping of statutory norms onto a specific commercial context, namely the processing of personal data by marketplace platforms. Three complementary approaches are used. The statutory approach is used to analyse the text of the UU PDP (Law Number 27 of 2022), its relationship to the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and the Consumer Protection Law (Law Number 8 of 1999), insofar as the latter continues to supply a complementary civil remedy for marketplace users. The conceptual approach is used to clarify key concepts, including personal data, data controller, data processor, and the preventive-repressive protection distinction drawn from Hadjon's legal-protection theory and the privacy theory of Westin. The case approach is used to examine the 2019 Bukalapak breach, the 2020 Tokopedia breach, and the associated civil lawsuit before the Central Jakarta District Court, as concrete illustrations against which the practical operation of the UU PDP's mechanisms, had they been in force at the relevant time, can be assessed.

Data for this study are secondary, gathered through library-based legal research. Primary legal materials comprise the applicable statutes and implementing regulations identified above. Secondary legal materials comprise Indonesian legal scholarship, journal

articles, and practitioner commentary addressing personal data protection, e-commerce consumer protection, and the specific documented breach incidents referenced in this study. The collected materials are analysed qualitatively using grammatical, systematic, and teleological interpretive techniques: the constituent elements of the relevant statutory rights and obligations are first isolated, then tested against the operational and commercial realities of the marketplace business model, including its reliance on third-party processors and standard-form consent mechanisms, in order to assess the practical adequacy of the resulting legal protection and to identify points at which formal entitlement and practical protection diverge.

RESULT AND DISCUSSION

Marketplace Platforms as Personal Data Controllers

Under the UU PDP, a marketplace operator that determines the purpose and means of processing users' personal data, such as deciding to collect delivery addresses for order fulfilment or browsing history for personalised recommendation, qualifies as a personal data controller and bears the corresponding statutory obligations directly, regardless of the platform's classification for other regulatory purposes, such as its status as an electronic system provider under the Electronic Information and Transactions Law or as a trading through electronic system operator under commerce regulation. This classification is significant because it confirms that a marketplace cannot discharge its personal data obligations merely by complying with general electronic-system security requirements; it must independently satisfy the UU PDP's more specific requirements concerning lawful basis, data subject rights facilitation, and breach notification. Where a marketplace engages third parties, such as independent sellers operating storefronts on the platform, courier and logistics partners, or payment gateway providers, to process user data for their own or shared purposes, the allocation of controller and processor status, and the corresponding allocation of liability, depends on the specific factual division of decision-making authority over the data in question, a determination the UU PDP leaves to be assessed case by case rather than through a fixed statutory presumption specific to marketplace structures.

Preventive Protection: Consent, Lawful Basis, and the Limits of Standard-Form Agreement

Assessed against Hadjon's preventive protection category, the UU PDP's requirement that processing rest on a valid lawful basis, most commonly consent or contractual necessity in the marketplace context, in principle requires platforms to identify and disclose the specific purpose of each category of data collected before processing begins, offering users an ex ante

opportunity to understand and, in the case of consent-based processing, to decline non-essential data uses. In practice, however, marketplace platforms in Indonesia, consistent with prevailing global industry practice, typically obtain this consent through a single, bundled acceptance of lengthy standard-form terms of service and privacy policy presented at account registration, a mechanism that satisfies the formal requirement of documented consent while providing limited practical opportunity for a typical user to read, understand, or negotiate the specific data uses to which they are consenting. This practice, sometimes described in privacy scholarship as consent fatigue or bundled consent, means that the preventive function of the UU PDP's consent requirement operates more robustly as a compliance and evidentiary safeguard for controllers than as a genuinely informed, granular choice mechanism for individual users, a gap the statute itself does not fully resolve, since it requires consent to be informed and specific in principle but does not prescribe a specific format, such as layered or just-in-time consent interfaces, that would meaningfully improve practical comprehension.

Preventive Protection: Security Obligations and Third-Party Processor Risk

A further preventive dimension concerns the UU PDP's requirement that controllers implement technical and organisational security measures appropriate to the risk of the processing undertaken. Applied retrospectively to the Tokopedia and Bukalapak incidents, this requirement would have obliged the platforms to maintain security measures commensurate with the scale and sensitivity of the tens of millions of user records each held, and a demonstrated security failure resulting in unauthorised access would, under the current framework, expose the controller to administrative sanction independent of any separate civil liability. The more structurally significant preventive challenge in the marketplace context, however, concerns the extended chain of third-party processors, couriers, payment gateways, and increasingly, third-party advertising and analytics providers integrated into marketplace platforms, each representing a potential point of failure through which user data can be exposed even where the primary marketplace controller's own systems remain secure. Because Article 20 requires only that the controller-processor relationship be governed by an agreement allocating compliance responsibility, without prescribing a specific minimum security standard applicable uniformly across the processing chain, the practical security of user data within the broader marketplace ecosystem depends significantly on the rigour of individual, privately negotiated data processing agreements, the content of which is not ordinarily visible to, or verifiable by, the individual data subject whose information is at stake.

Repressive Protection: The Breach Notification Duty as a New Accountability Mechanism

The most significant repressive innovation the UU PDP introduces, relative to the pre-2022 framework under which the Tokopedia and Bukalapak breaches occurred, is the mandatory seventy-two-hour breach notification duty under Article 46. Prior to the UU PDP, affected users' awareness of the Tokopedia and Bukalapak breaches depended substantially on public disclosure through media reporting and the platforms' own discretionary public relations response, rather than on any binding legal obligation to notify affected individuals within a defined timeframe or with defined minimum content. Under the current framework, a comparable breach would trigger a binding obligation to notify both affected users and the Personal Data Protection Supervisory Authority within seventy-two hours, specifying the categories of data exposed, the circumstances of the failure, and the remedial steps taken, converting what was previously a matter of platform discretion and public pressure into an enforceable legal duty whose breach independently exposes the controller to administrative sanction. This represents a meaningful strengthening of repressive protection in the specific sense of ensuring timely user awareness, which in turn enables affected individuals to take protective measures, such as changing compromised passwords or monitoring for identity-based fraud, more promptly than was possible under the previous disclosure-by-discretion model.

Repressive Protection: Administrative, Criminal, and Civil Avenues Compared

The UU PDP's layered sanctions regime gives marketplace users three theoretically available repressive avenues following a violation: administrative sanction pursued by the Personal Data Protection Supervisory Authority against the controller, which can include a fine of up to two percent of annual revenue but which primarily vindicates regulatory compliance rather than compensating the individual user directly; criminal prosecution under Articles 67 and 68, which targets the individual perpetrator of unlawful collection, disclosure, use, or falsification of personal data, and which, where a corporation is implicated, can extend liability to management and controlling persons under Article 70; and civil compensation claims, which the UU PDP's Article 12 confirms as an entitlement of the data subject and which remain the primary avenue through which an individual user can seek direct financial redress for harm suffered, as illustrated by the Komunitas Konsumen Indonesia lawsuit against Tokopedia. Comparing these three avenues, the administrative and criminal mechanisms offer stronger general deterrence against future non-compliance and, in the criminal case, target culpable individual and corporate misconduct directly, but neither delivers individualised compensation to affected users as such; only the civil avenue does so, and civil litigation, as the protracted and evidentially demanding history of the Tokopedia lawsuit illustrates, remains comparatively

slow and resource-intensive relative to the scale of harm typically suffered by any single affected user in a mass data breach, whose individual loss, absent proof of concrete financial fraud traceable to the breach, may be difficult to quantify in a manner that justifies the cost of individual litigation.

The Institutional Gap: Supervisory Authority Capacity

A recurring theme in commentary on the UU PDP's practical implementation concerns the institutional capacity of the Personal Data Protection Supervisory Authority itself. The statute contemplates an authority with functions spanning policy formulation, compliance supervision, administrative enforcement, and facilitation of out-of-court dispute resolution across every sector of the Indonesian economy, a mandate of considerable breadth relative to the institution's comparatively recent establishment and the scale of the digital economy it is tasked with supervising, of which the marketplace sector, given its concentration of personal data and its large user base, represents a particularly high-priority segment. Until the supervisory authority develops sector-specific technical guidance, a track record of enforcement action, and sufficient staffing to conduct proactive compliance audits rather than relying solely on complaint-driven investigation, marketplace platforms' practical compliance incentives will continue to be shaped as much by reputational risk and civil litigation exposure, of the kind demonstrated in the Tokopedia case, as by anticipated regulatory enforcement, a dynamic that somewhat mirrors, in the personal data domain, the enforcement capacity challenges observed in other areas of Indonesian regulatory practice.

Cross-Border Data Transfer and Cloud Infrastructure

Many Indonesian marketplace platforms rely on cloud computing infrastructure operated by providers with data centres located outside Indonesia, meaning that user personal data collected domestically is frequently transferred to or processed on servers located abroad as a routine matter of technical architecture rather than as an exceptional transaction. Article 56 of the UU PDP permits cross-border transfer of personal data where the receiving country maintains a data protection standard equivalent to or higher than that of Indonesia, or, failing such equivalence, where the controllers involved provide adequate and binding safeguards or obtain the data subject's consent. Because a formal, published determination of which specific countries satisfy the equivalence standard has not been comprehensively established for all jurisdictions in which marketplace cloud infrastructure is commonly located, platforms in practice often rely on the binding corporate safeguard or consent bases instead, a workable but comparatively less certain compliance pathway that leaves open a degree of interpretive risk regarding the adequacy of specific contractual safeguards, particularly for smaller marketplace

operators without the negotiating leverage to secure detailed data protection commitments from large multinational cloud service providers.

Children's Data and Vulnerable User Categories

Marketplace platforms are, as a matter of ordinary commercial practice, not restricted to adult users, and delivery, gift purchase, and family shared-account arrangements mean that a marketplace's personal data holdings not infrequently include information relating to minors, whether as named recipients of deliveries or as users of accounts nominally registered to an adult household member. The UU PDP classifies children's data as specific personal data requiring heightened protection and, under Article 21, requires parental or guardian consent for the processing of a child's personal data. Marketplace platforms do not, as a general matter, operate dedicated verification mechanisms capable of reliably distinguishing a minor user or delivery recipient from an adult one, meaning that compliance with the heightened children's data protection standard in practice depends substantially on self-reported account information of uncertain reliability, an implementation gap that mirrors similar age-verification challenges observed across the broader digital services sector rather than one unique to marketplace platforms specifically, but one that nonetheless represents an area where the formal statutory protection significantly exceeds current practical enforceability.

Synthesis: A Strengthened but Incompletely Realised Protective Framework

Read together, the preceding analysis indicates that the UU PDP meaningfully strengthens both the preventive and repressive dimensions of legal protection available to marketplace users relative to the fragmented pre-2022 framework, most concretely through the codified catalogue of data subject rights, the mandatory lawful-basis and security obligations imposed on controllers, the binding seventy-two-hour breach notification duty, and the availability of administrative and criminal sanctions alongside the pre-existing civil remedy. At the same time, the practical realisation of this strengthened framework remains incomplete in specific, identifiable respects: preventive consent mechanisms continue to operate largely through low-comprehension standard-form agreements, security assurance across the extended third-party processor chain depends on privately negotiated arrangements not visible to individual users, the supervisory authority's enforcement capacity is still developing relative to the scale of the sector it oversees, cross-border transfer compliance pathways carry residual interpretive uncertainty, and children's data protection depends on self-reported information of uncertain reliability. None of these gaps reflects a deficiency in the UU PDP's substantive text as such; rather, each reflects the structural distance between a comprehensive statutory entitlement and the institutional, technical, and market conditions required to make that

entitlement fully operative in the specific commercial environment of a large-scale online marketplace.

Comparative Note: Aligning Marketplace Practice with International Standards

Indonesian data protection scholarship frequently situates the UU PDP against the European Union's General Data Protection Regulation as a comparative reference point, and this comparison is instructive for the marketplace context specifically. The General Data Protection Regulation's layered and granular consent requirements, its data protection by design and by default principle, and its established body of regulatory guidance on permissible cookie and tracking practices offer a more developed template than currently exists in Indonesian implementing regulation for translating the UU PDP's general consent and security principles into specific, auditable marketplace platform practices. Because the UU PDP was deliberately drafted at a comparable level of principle-based generality to allow application across highly diverse sectors, from banking to healthcare to retail, sector-specific technical guidance addressing marketplace practices in particular, such as acceptable standards for presenting layered consent at account registration, permissible retention periods for transaction and browsing history, and minimum security expectations for integrated payment and logistics data sharing, remains an area where Indonesia's regulatory framework could productively continue to develop, drawing on comparative experience without displacing the UU PDP's own statutory architecture.

This comparative observation also underscores a broader point relevant to the overall assessment offered in this article: the effectiveness of marketplace personal data protection in Indonesia will depend substantially on the pace and quality of subordinate regulation and supervisory guidance issued under the UU PDP over the years following its enactment, rather than on the text of the statute alone, since a principle-based framework of this kind necessarily leaves considerable interpretive space for sector-specific elaboration. Continued academic and regulatory attention to the marketplace sector specifically, given its scale, its concentration of sensitive financial and behavioural data, and its documented history of major breach incidents, is accordingly warranted as Indonesia's data protection framework continues to mature.

Practical Recommendations for Marketplace Compliance

Translating the preceding analysis into practical guidance, marketplace platforms seeking to strengthen genuine, rather than merely formal, compliance with the UU PDP should consider several concrete measures beyond minimum statutory adherence. First, platforms should move progressively from single bundled consent screens toward layered consent interfaces that separately present essential processing, necessary for order fulfilment and

payment, from optional secondary uses, such as targeted advertising and cross-platform data sharing, allowing users to decline the latter without losing access to core marketplace functionality. Second, platforms should maintain a current, centrally accessible inventory of all third-party processors with access to user personal data, including logistics, payment, and advertising partners, together with the specific categories of data each processor receives, both to facilitate the platform's own compliance verification and to support timely and accurate breach notification should an incident occur within any part of the extended processing chain. Third, platforms should establish internal incident response procedures capable of identifying, assessing, and notifying a personal data breach within the seventy-two-hour window Article 46 requires, recognising that the technical complexity of tracing a breach's scope across a multi-party processing ecosystem can consume much of that window if response procedures are not established and rehearsed in advance. Fourth, platforms operating cross-border cloud infrastructure should proactively document the specific legal basis, whether adequacy, contractual safeguard, or consent, relied upon for each material cross-border transfer, given the residual interpretive uncertainty identified in this study's discussion of Article 56. Adopting these measures would help close the gap this study has identified between the UU PDP's substantial formal entitlements and their practical realisation within the specific operational context of Indonesia's marketplace sector.

CONCLUSION

This study finds that Law Number 27 of 2022 concerning Personal Data Protection provides marketplace users in Indonesia with a substantially more comprehensive framework of legal protection than existed at the time of the widely documented Bukalapak and Tokopedia data breaches, converting what were previously discretionary platform responses and slow, evidentially demanding civil claims into a structured regime of codified data subject rights, binding controller obligations, a mandatory time-bound breach notification duty, and a layered system of administrative, criminal, and civil accountability. Applying Hadjon's preventive-repressive framework, the UU PDP strengthens preventive protection through its lawful-basis and security-obligation requirements, and strengthens repressive protection most significantly through the breach notification duty and the newly available administrative and criminal enforcement avenues operating alongside civil compensation claims.

Nonetheless, the practical adequacy of this protection remains constrained by factors that further legislative refinement and institutional development, rather than the current statutory text alone, must address: the persistence of low-comprehension, bundled consent

mechanisms in marketplace terms of service; the opacity of security practices across extended third-party logistics, payment, and advertising processor chains; the still-developing enforcement capacity of the Personal Data Protection Supervisory Authority relative to the scale of the marketplace sector; residual uncertainty surrounding cross-border data transfer compliance pathways; and the practical unreliability of self-reported information as a basis for enforcing heightened protection of children's data. Addressing these gaps calls for sector-specific implementing regulation tailored to electronic commerce, regulatory guidance clarifying acceptable standards for layered or just-in-time consent presentation, strengthened supervisory authority capacity for proactive compliance auditing of high-volume data controllers such as major marketplace platforms, and continued judicial and regulatory attention to civil compensation mechanisms capable of delivering meaningful individual redress in mass data breach scenarios. Pursued together, these measures would move Indonesia's marketplace personal data protection framework from a substantially strengthened statutory entitlement toward a more fully realised practical safeguard for the millions of Indonesian consumers who transact through online marketplaces daily.

REFERENCES

- Ejournal APPIHI. "Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi terhadap Tanggung Jawab Platform E-Commerce."
- Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: PT Bina Ilmu.
- Hukumonline. "Ancaman Sanksi Administratif Hingga Pidana dalam UU Pelindungan Data Pribadi." hukumonline.com.
- Indonesia Baik. "Ragam Ancaman Pidana Perlindungan Data Pribadi." indonesiabaik.id.
- JDIH Kota Probolinggo. "Penanganan Kebocoran Data Pribadi Pelanggan e-Commerce." jdih.probolingkokota.go.id.
- Jurnal Kajian Hukum Dan Kebijakan Publik. "Perlindungan Hukum Bagi Pengguna Aplikasi Tokopedia Dari Kebocoran Data Pribadi." Vol. 2, No. 2, Januari-Juni 2025.
- Jurnal Kajian Hukum Dan Kebijakan Publik. "Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022."
- Jurnal Program Pascasarjana Ilmu Hukum VERITAS. "Pengaturan Perlindungan Data Pribadi Konsumen Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." Vol. 10, No. 1 (2024).
- Kementerian Komunikasi dan Informatika. *Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik*.
- Kompas.com. "UU Perlindungan Data Pribadi: Jenis Data dan Sanksi Pidananya." nasional.kompas.com.
- Kompas.id. "UU Pelindungan Data Pribadi Akhirnya Disahkan, Asa Baru Mencegah Kebocoran Data." kompas.id, 19 Oktober 2022.
- Peraturan BPK. "UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi." peraturan.bpk.go.id.
-

- Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).
- Republik Indonesia. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821).
- RIGGS: Journal of Artificial Intelligence and Digital Business. "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi." Vol. 4, No. 3 (2025).
- Rumah Tahanan Negara Kelas IIB Pelaihari. "4 Tindak Pidana Dalam UU PDP dan Sanksinya." sippn.menpan.go.id.
- SIP Law Firm. "Perlindungan Data Pribadi Konsumen dalam E-Commerce: Kewajiban, Hak, dan Tanggung Jawab." siplawfirm.id.
- SIP Law Firm. "Sanksi Hukum Dalam Undang-Undang Perlindungan Data Pribadi." siplawfirm.id.
- The Conversation Indonesia. "Tokopedia dan Bukalapak memang bisa digugat, tapi tidak lantas masalah kebocoran data tuntas." theconversation.com.
- Tirto.id. "Isi UU Perlindungan Data Pribadi Undang-Undang No 27 Tahun 2022." tirto.id.
- Universitas Islam Indonesia, Repositori Digilib. "Tanggung Jawab PT Tokopedia dalam Kasus Kebocoran Data Pribadi Pengguna." dspace.uui.ac.id.
- Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review*, Vol. 4, No. 5 (1890).
- Westin, Alan F. *Privacy and Freedom*. New York: Atheneum.