EISSN: 2622-9668|PISSN: 2622-982X
Volume 9 Nomor 2 Agustus 2026: 407-442
DOI: 10.30996/jhbbc.v9i2.133200
Jurnal Hukum Bisnis Bonum Commune

Digital Contracts and Personal Data Protection: Indonesia's Experience after the Personal Data Protection Law

Admiral[1*], Ridwan Arifin[2], Sergi Fernandez Alejandro[3], Valerio Sebastian[4]
[1]Universitas Islam Riau, Indonesia
[2]Universitas Negeri Semarang, Indonesia
[3,4] Sociedad Civil de Derecho y Políticas Públicas, Spain
[*]Corresponding Author: admiral@law.uir.ac.id

Article History:
Submitted:
25-01-2026
Received:
20-02-2026
Accepted:
15-07-2026

Keywords:
digital contracts; personal data protection; consent; platform economy; indonesia

Abstract

The rapid expansion of the digital economy has intensified the use of digital contracts as primary instruments governing interactions between platform providers and users, particularly in relation to the collection and processing of personal data. In Indonesia, this development has gained renewed legal significance following the enactment of Law No. 27/2022. This article examines how the new legal framework reshapes the relationship between digital contracts and personal data protection, with a particular focus on the role of consent in digital contracting practices. Employing doctrinal legal research and regulatory analysis, the study explores the extent to which digital contracts comply with the substantive requirements of lawful data processing under Law No. 27/2022. The analysis demonstrates that, despite strengthened statutory protections, digital contracts, often presented as standard form or clickwrap agreements, continue to rely heavily on formalistic consent mechanisms that may undermine users' effective control over their personal data. The article argues that the persistence of imbalanced bargaining power and opaque contractual terms poses significant challenges to the realization of meaningful consent, as envisioned by the new law. By situating Indonesia's experience within broader debates on data governance and digital contracting, this study contributes to the understanding of how personal data protection regimes operate in emerging digital markets. The findings highlight the need for a more integrated regulatory approach that aligns contract law principles with data protection norms to ensure both legal certainty and substantive fairness in digital transactions. The article concludes by offering reflections relevant to other Southeast Asian jurisdictions facing similar regulatory challenges.

1. Introduction

The rapid expansion of platform-based economies has fundamentally transformed contractual relations in contemporary societies.[1] Digital platforms operating in sectors such as e-commerce, transportation, financial technology, health services, and social media increasingly rely on digital contracts as the primary legal instruments governing interactions with users.[2] These contracts—commonly manifested as clickwrap or browsewrap agreements—are not limited to regulating access to services; they function as key legal mechanisms through which platforms legitimize the large-scale collection, processing, and

[1]Antonio Orti Vallejo, "Contractual relationships in collaborative economy platforms." *European Review of Private Law* 27, no. 5 (2019): 995-1022. Martin Kenney, and John Zysman. "The Rise of the Platform Economy." *Issues in Science and Technology* 32, no. 3 (2016): 61-69.
[2]Gustavo Guarín Duque, and Julián David Zuluaga Torres. "Enhancing E-commerce through blockchain (DLTs): the regulatory paradox for digital governance." *Global Jurist* 20, no. 2 (2020): 20190049.

commercialization of personal data.[3] As a result, digital contracts have become central to the governance of personal data in the digital economy.[4]

Indonesia represents a particularly significant context for examining this phenomenon. As one of Southeast Asia's largest digital markets, Indonesia has experienced rapid growth in internet penetration, mobile usage, and platform adoption.[5] Digital platforms routinely collect extensive categories of personal data, including identity information, financial data, location data, and behavioral profiles.[6] In practice, user consent to such data processing is almost exclusively obtained through standardized digital contracts that are non-negotiable and presented on a take-it-or-leave-it basis.[7] Socio-legal studies and regulatory reports consistently indicate that users rarely read or fully comprehend these contractual terms, raising serious questions about the substantive validity of consent in digital transactions.

These concerns are amplified by a series of high-profile personal data breaches that have occurred in Indonesia in recent years. Cases involving major digital platforms and public service providers—such as the data breaches affecting Tokopedia and BPJS Kesehatan—have exposed millions of users' personal data and revealed systemic weaknesses in data governance and accountability.[8] Notably, in these cases, users had formally agreed to digital contracts authorizing data processing, yet such consent offered little protection against misuse, security failures, or delayed regulatory responses. These incidents underscore a structural gap between formal contractual consent and the effective protection of personal data in practice.

The enactment of Indonesia's Personal Data Protection Law (Law Number 27 of 2022 concerning Personal Data Protection (Law No. 27/2022)) marks a significant regulatory intervention aimed at addressing these challenges. The law introduces comprehensive

---

[3]Wayne Barnes, "Online Disinhibited Contracts." *Pepperdine Law Review* 51, no. 2 (2024): 267-324.

[4]Admiral Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." *Lex Scientia Law Review* 7, no. 2 (2023): 995-1048; Admiral Admiral, et al. "Indonesia's Online Loan Challenges: What Legal Actions Can Solve the Most Pressing Issues?." *Indonesian Journal of Legal Community Engagement* 8, no. 1 (2025): 275-314; Rosyidi Hamzah, et al. "Imperfect Information of Bankers Clause in Credit Agreements in Banking Institutions: Further Legal Impact." *Lex Scientia Law Review* 7, no. 2 (2023): 529-568; Admiral Admiral, et al. "Unfair Terms in Standard Digital Contracts: A Hidden Threat to Human Rights and Consumer Justice." *Yustisia* 14, no. 3 (2025): 312-340; Bambang Adji Pamungkas. "Feminist Legal Critique of Child Marriage Dispensation Practices in Indonesian Religious Courts." *The Indonesian Journal of Feminist Legal Studies* 1, no. 1 (2026): 31-60.

[5]*See* Edwin Jurriëns, and Ross Tapsell. "Challenges and opportunities of the digital 'revolution' in Indonesia." *Digital Indonesia: Connectivity and Divergence* 2020 (2017): 275-288; Anggia Putri Lestari, Syahla Amany Fatiha, and Sylvia Octa Putri. "E-Commerce in Indonesia's Economic Transformation and Its Influence on Global Trade." *International Journal of Computer in Law & Political Science* 4 (2024): 10-23.

[6]*See* Lupton, Deborah. "Personal data practices in the age of lively data." *Digital Sociologies*. Policy Press, 2017, pp. 339-354.

[7]Ifeoma Ajunwa, and Austin Kamer. "Data Privacy by Contract." *Cardozo Law Review* 45, no. 5 (2024): 1436-1491.

[8]Nofie Iman, "The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms." *International Journal of Law and Management* 66, no. 6 (2024): 774-791; Wahyu Nandang Irmawan, et al. "Human Rights in the Digital Age: The Indonesian Judiciary's Response to Internet Censorship and Privacy Laws." *Indonesian Court and Justice Review* 2, no. 3 (2025); Fayhan Rafiq Alamsyah, and David Wilson. "The Role of Digital Economy in Promoting Economic Justice: A Case Study of Indonesia's Tech Sector." *Indonesian Economic Justice Review* 1, no. 4 (2024).

principles governing lawful data processing, strengthens data subject rights, and imposes explicit obligations on data controllers and processors.[9] Importantly, it seeks to recalibrate the role of consent by emphasizing transparency, voluntariness, purpose limitation, and accountability. However, the implementation of these principles occurs within a legal environment still shaped by classical contract law doctrines that prioritize freedom of contract and formal agreement, even in highly asymmetrical digital market contexts.[10] This regulatory configuration creates a fundamental tension. While Law No. 27/2022 aspires to enhance substantive data protection, digital contracts continue to operate as instruments of private ordering that consolidate platform power and normalize broad data extraction practices.[11] Consent, in this setting, risks functioning less as a mechanism of individual autonomy and more as a legal fiction that legitimizes data-intensive business models. This tension raises critical questions about whether data protection objectives can be realized without a deeper reconsideration of the contractual foundations of digital governance.[12]

Against this condition, this article critically examines the interaction between digital contracts and personal data protection in Indonesia following the enactment of Law No. 27/2022. It addresses the following research questions: to what extent do prevailing digital contracting practices comply with the substantive consent standards mandated by the new law? How do power imbalances, standardization, and platform dominance affect the realization of data subject rights? And what regulatory strategies are necessary to reconcile contract law with data protection norms in emerging digital economies?

This article makes three critical contributions**.** *First*, it challenges the dominant assumption that contractual consent in digital environments is inherently compatible with data protection objectives, demonstrating how consent is often formalistic and structurally constrained. *Second*, it advances a socio-legal understanding of digital contracts as instruments of data governance rather than neutral legal tools, highlighting their role in shaping power

[9]Tegar Islami Putra, et al. "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study." *Unnes Law Journal* 10, no. 2 (2024): 223-254; Supeno Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal. "Personal Data Protection in Review of Legal Theories and Principles." *Journal of Law and Legal Reform* 6, no. 3 (2025): 1349-1376; Ardhitama Sucahyanto. "Digital Society and the Transformation of Community-Based Dispute Resolution in Indonesia." *The Indonesian Journal of Sociolegal Development* 1, no. 1 (2026): 31-60.

[10] Tegar Islami Putra, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis. "Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection." *The Indonesian Journal of International Clinical Legal Education* 7, no. 2 (2025): 203-234; Firsta Rahadatul 'Aisy, Muhammad Azil Maskur, and A. M. Adzkiya 'Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore." *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431-482; Arnanda Yusliwidaka, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?." *Pandecta Research Law Journal* 19, no. 2 (2024): 173-202.

[11]*See further* Mark Burdon, *Digital Data Collection and Information Privacy Law*. Vol. 54. Cambridge University Press, 2020.

[12]Felix Pratama Tjipto, "Comparative Law Analysis of Consumer Protection Law in E-Commerce Transaction Between Indonesia and United States." *UIR Law Review* 5, no. 2 (2021): 11-25; Sawitri Yuli Hartati, Emelia Kontesa, and Agri Baskara. "Sharia fintech in the digital age: Human Rights in Sharia Fintech Through Criminal Law Safeguards." *Indonesian Journal of Criminal Law Studies* 8, no. 2 (2023): 289-314.

relations between platforms and users. *Third*, by situating Indonesia's experience within broader debates on data protection and platform regulation, the article contributes insights relevant to other Southeast Asian jurisdictions and emerging digital markets facing similar regulatory dilemmas.

2. Methods

This study employs a doctrinal legal research approach to examine the interaction between digital contracts and Law No. 27/2022. Doctrinal analysis focuses on the interpretation and application of statutory provisions, regulations, and judicial decisions related to digital contracting and personal data protection. Key sources include Law No. 27/2022, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (Law No. 19/2016), implementing regulations, and relevant ministerial guidelines. The analysis identifies legal standards governing consent, transparency, and accountability, and examines how these rules interface with existing digital contracting practices in Indonesia.

In addition to doctrinal research, the study adopts a socio-legal perspective to contextualize legal rules[13] within the practical realities of digital platform usage. This includes examining publicly reported data breaches, enforcement cases, and empirical studies concerning user engagement with digital contracts. For instance, incidents such as the Tokopedia[14] and BPJS Kesehatan[15] breaches provide concrete evidence of how formal consent in digital contracts can fail to protect users' personal data. The socio-legal approach also considers power asymmetries between platform providers and users, highlighting structural inequalities that influence the effectiveness of consent as a regulatory tool. By integrating doctrinal and socio-legal insights, the study situates the law within the broader socio-technical and economic environment of Indonesia's digital economy.

The study incorporates a comparative and critical lens by drawing on experiences from other Southeast Asian jurisdictions and international best practices. This includes analysis of ASEAN frameworks, Singapore's Personal Data Protection Act, and global standards such as the EU General Data Protection Regulation (GDPR), to evaluate the sufficiency of Indonesia's regulatory approach. The critical dimension emphasizes not only compliance with statutory requirements but also the substantive realization of data protection principles in practice. By combining doctrinal, socio-legal, and comparative analyses, the study provides a comprehensive understanding of digital contracts as instruments of data governance and

[13]*See* Reza Banakar, and Max Travers, eds. *Theory and Method in Socio-Legal Research*. Bloomsbury Publishing, 2005; Naomi Creutzfeldt, Marc Mason, and Kirsten McConnachie. "Socio-Legal Theory and Methods: Introduction." *Routledge Handbook of Socio-Legal Theory and Methods*. London: Routledge, 2019, pp. 3-8.

[14]*See* Ivan Taffarel Almeyda, and Endang Prasetyawati. "Consumer protection for the hacking of personal data of tokopedia marketplace users." *Journal Evidence of Law* 3, no. 2 (2024): 206-219; Elfian Fauzy, and Annisa Hafizhah. "Legal analysis of user personal data leak cases at tokopedia." *Mahadi: Indonesia Journal of Law* 2, no. 1 (2023): 41-52.

[15]One Maulida, and Hari Utomo. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna dalam Perspektif Hukum Pidana." *Indonesian Journal of Law and Justice* 1, no. 2 (2023): 1-9; Muhammad Raihan Faiqy, et al. "Urgensi Realisasi Peran Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi." *Padjadjaran Law Review* 10, no. 1 (2022): 142-156.

identifies challenges and opportunities for improving legal and regulatory frameworks in Indonesia and the broader region.

3. Results and Discussion

3.1. Digital Contracts in the Indonesian Digital Economy

Digital contracts have become the primary mechanism through which platform-based economies regulate interactions between service providers and users. Broadly, digital contracts are electronic agreements concluded through online platforms and interfaces, which users must accept to access services.[16] These contracts typically take the form of clickwrap agreements, where users actively click an "*I agree*" button; browsewrap agreements, where continued use of a website or platform is construed as acceptance; and standard form contracts, which are pre-drafted with minimal room for negotiation. While these contracts enable platforms to operate efficiently at scale, they also raise critical questions about the meaningfulness of user consent, comprehension, and the equitable distribution of rights in digital spaces.

In Indonesia, digital contracts are widely employed across a rapidly expanding digital economy. E-commerce platforms such as Tokopedia and Bukalapak, ride-hailing services like Gojek and Grab, fintech companies, and online health platforms rely heavily on standardized electronic contracts to regulate user behavior, allocate liability, and govern data collection practices.[17] The adoption of these contracts reflects both operational efficiency and the formal legal recognition of electronic agreements under Indonesian law. Nevertheless, the predominance of take-it-or-leave-it terms limits user autonomy, creating significant imbalances in bargaining power between platforms and consumers.

The standardization of digital contracts reinforces power asymmetries in favor of platform providers. Users are often presented with lengthy, complex terms of service and privacy policies, which empirical studies suggest are rarely read or fully understood.[18] Such imbalances raise concerns about whether consent obtained through digital contracts is genuinely informed or merely formalistic. High-profile data breaches—such as the Tokopedia breach in 2020, affecting approximately 91 million user accounts[19], and the BPJS Kesehatan breach in 2022[20]—illustrate the potential consequences of these imbalances, where formal agreement to contract terms did not translate into meaningful protection of personal data.

---

[16]Matteo Ortino, "The Functions of Law and of Digital Platforms in the Payment System." *European Business Law Review* 33, no. 7 (2022): 1083-1107.

[17]Jessica Basukie, Yichuan Wang, and Shuyang Li. "Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets." *Technological Forecasting and Social Change* 161 (2020): 120310.

[18]Florian Möslein, "Digitized terms: the regulation of standard contract terms in the digital age." *European Review of Contract Law* 19, no. 4 (2023): 300-320.

[19]Yudha Gaizka Putra, and Adhining Prabawati Rahmahani. "Legal Protection for Victims of Personal Data Leakage (Case Study on Victims of PT Tokopedia in 2020)." *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy* 1, no. 1 (2025): 600-612; Ivan Taffarel Almeyda, and Endang Prasetyawati. "Consumer protection for the hacking of personal data of tokopedia marketplace users." *Journal Evidence of Law* 3, no. 2 (2024): 206-219.

[20]Cinda Sorisa, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." *Journal Sains Student Research* 2, no. 6 (2024): 586-593; Ridho Rivantoro, and Dyah Permata Budi Asri. "Tanggung Jawab Hukum Korporasi Atas Kebocoran

The legal foundation for digital contracts in Indonesia derives from multiple sources. Under Article 1320 of the Civil Code (KUHPer), a contract is valid if it meets four conditions: mutual agreement, legal capacity, lawful object, and lawful cause.[21] Law No. 19/2016[22] further recognizes electronic contracts as legally binding under Articles 11 and 12, equating electronic signatures and communications with traditional written forms, provided authenticity and integrity requirements are met.[23] This doctrinal framework legitimizes electronic contracting but primarily focuses on formal validity rather than the substantive fairness or power dynamics inherent in digital agreements.

Operationalization of electronic contracts is further guided by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (Government Regulation No. 71/2019), which establishes standards for electronic documents and information systems, including digital platforms. These provisions govern the technical and procedural aspects of contract formation, authentication, and retention.[24] While they

---

Data Peserta BPJS Kesehatan Berdasarkan UU No. 27 Tahun 2022: Penelitian." *Jurnal Pengabdian Masyarakat dan Riset Pendidikan* 4, no. 3 (2026): 16034-16040.

[21]Natasya Yunita Sugiastuti, and Dian Purnamasari. "Improvement of Substantive Provisions of the Validity of Agreement in the Indonesian Civil Code." *Diponegoro Law Review* 8, no. 1 (2023): 124-140; Ery Agus Priyono, Budiharto Budiharto, and Asri Hayyunniarizka Wulandari. "Regulations for E-Commerce Agreement According to ICT Act and Title III of Indonesian Civil Code." *Diponegoro Law Review* 4, no. 1 (2019): 76-88.

[22]However, articles 11 and 12 of Indonesia's Electronic Information and Transactions Law (as amended by Law No. 19 of 2016) face several practical problems and challenges in their implementation. Although Article 11 formally recognizes the legal validity of electronic signatures, its use of broad and vague terms such as "certain methods" for identification and consent creates legal uncertainty and allows multiple interpretations, especially regarding non-certified electronic signatures. In practice, courts often still treat electronic signatures with caution, requiring technical proof and expert testimony, which makes enforcement costly and complex. Article 12, which places an obligation on all parties to secure electronic signatures, also presents challenges because it does not clearly define minimum security standards, thereby shifting a heavy burden of responsibility onto users who may lack sufficient digital literacy. This situation is further complicated by increasing cybercrime risks, such as identity theft and unauthorized access, as well as uneven understanding of electronic evidence among law-enforcement authorities. As a result, while these articles provide an essential legal foundation for electronic transactions, their effectiveness is constrained by ambiguity, technological dependency, and gaps in legal and digital capacity. *See also* Adi Putra Manggala, et al. "Legal Review of the Implementation of Electronic Contracts and Protection of Parties in Digital Transactions in Indonesia." *International Journal of Service Science, Management, Engineering, and Technology* 8, no. 1 (2025): 1-8; Syarifah Lisa Andriati, and Dinda Aprilia Batubara. "The Validity of QR-Code Digital Signature in Contract Towards the Evidence Agenda in Civil Court." *Mahadi: Indonesia Journal of Law* 3, no. 2 (2024): 95-102.

[23]Muhammad Rizky Aji Perdana, Rizki Tri Anugrah Bhakti, and Dwi Afni Maileni. "Validity of Electronic Signatures in Digital Agreements: An Analysis of the Application of the Intellectual Property Law and the Civil Code in E-Commerce Transactions." *Jurnal Mahkamah: Kajian Ilmu Hukum dan Hukum Islam* (2025): 565-578; Agnes Maria Janni Widyawati, Mig Irianto Legowo, and Heri Purnomo. "The Validity of Electronic Agreements in the Perspective of Indonesian Civil Law." *International Journal of Health, Economics, and Social Sciences (IJHESS)* 7, no. 2 (2025): 749-753.

[24]Hellen S. De Lima, Jupryanto Purba, and Diana Napitupulu. "Analisis Hukum Kontrak dalam Sistem Hukum Indonesia: Perlindungan, Wanprestasi, dan Tantangan Era Digital." *Jurnal Hukum Sasana* 11, no. 1 (2025): 190-204; Ditiya Salsabila, and Budi Ispriyarso. "Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif di Indonesia." *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam* 5, no. 2 (2023): 1343-1354.

enhance legal certainty for platforms, the regulations do not address socio-legal concerns such as information asymmetry, user comprehension, or the potential for exploitation in standardized contracts—issues that are critical when personal data is at stake.

The enactment of Law No. 27/2022 represents a significant attempt to address these gaps. Articles 12–17 emphasize that consent must be specific, informed, voluntary, and revocable, and require transparency regarding the purpose, retention, and potential transfer of personal data[25]. However, the law operates within a pre-existing digital contracting environment where consent is frequently formalistic. The interaction between traditional electronic contract frameworks and the substantive requirements of Law No. 27/2022 is thus complex, leaving unresolved questions about enforceability, accountability, and whether users can effectively exercise their data rights within the prevailing platform-driven contracting ecosystem.

In addition, Indonesia's legal framework on electronic contracts, particularly under Article 18 of Law Number 11 of 2008 concerning Electronic Information and Transactions (Law No. 11/2008), as amended by Law Number 1 of 2024, and Government Regulation No. 71/2019, adopts a predominantly formalistic approach to digital contracting. Article 18 of the Law No. 11/2008 recognizes the legal validity and binding force of electronic contracts, while Articles 46–52 of Government Regulation No. 71/2019 prescribe the minimum requirements for valid electronic contracts, including the identity of the parties, contractual object, terms and conditions, and mechanisms for acceptance. These provisions primarily aim to ensure legal certainty by establishing the validity, authenticity, and evidentiary value of electronic agreements. However, they largely replicate the traditional principles of contract law without sufficiently accounting for the distinctive characteristics of platform-based digital transactions.

This formalistic orientation leaves significant regulatory gaps in addressing substantive fairness within Indonesia's digital economy. Although Government Regulation No. 71/2019 requires electronic system operators to provide complete and accurate information, it does not impose meaningful obligations to ensure that users genuinely understand standard-form contracts or the consequences of consenting to extensive data processing practices. Likewise, neither Article 18 of the Law No. 11/2008 nor Articles 46–52 of Government Regulation No. 71/2019 require transparency regarding algorithmic decision-making, automated pricing, personalized contract terms, or profiling mechanisms that increasingly determine consumers' contractual experiences. The existing legal framework, therefore, continues to rely on the paradigm of conventional transactions, where contracting parties are assumed to possess relatively equal bargaining power and information. In reality, digital platforms operate through structural asymmetries created by data accumulation, algorithmic governance, and non-negotiable standard contracts. Consequently, the Indonesian regulatory framework should evolve beyond merely validating electronic contracts toward incorporating substantive

[25]Loso Judijanto, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights* 3, no. 1 (2024): 20-29; Tegar Islami Putra, et al. "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study." *Unnes Law Journal* 10, no. 2 (2024): 223-254; Suraji Suraji, and Ipop Abdi Prabowo. "Harmonizing Privacy Rights Protection in Electronic Transaction with Roscoe Pound's Legal Principle." *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 71-94.

principles of fairness, informed consent, and algorithmic transparency that are better suited to the realities of the contemporary digital economy.

The combination of formal legal recognition and practical standardization positions digital contracts as instruments of private governance rather than neutral legal tools. While the Law No. 27/2022 introduces normative principles designed to protect data subjects, socio-legal realities—such as take-it-or-leave-it contracts, opaque terms, and significant information asymmetries—limit the realization of these protections. Digital contracts, in practice, often function to legitimize extensive data extraction and platform control, raising critical questions about the alignment of contract law, personal data protection, and substantive user autonomy. This tension forms the foundation for the subsequent analysis of consent under Law No. 27/2022, highlighting the necessity of a regulatory approach that integrates doctrinal rules with socio-legal realities.

3.2. The Transformation of Consent after Law No. 27/2022

The enactment of Law No. 27/2022 represents an important regulatory development in the governance of personal data within Southeast Asia. The law introduces comprehensive provisions governing the collection, storage, processing, and transfer of personal data, reflecting global trends toward recognizing data privacy as a fundamental right. Scholars such as Gillis and Simons[26] and Cate[27] have argued that personal data protection is not merely a regulatory compliance issue but a mechanism to rebalance asymmetrical power relations between institutions and individuals. In Indonesia, Law No. 27/2022 situates consent as a central pillar of data protection, explicitly linking individual autonomy with the responsibilities of data controllers and processors.[28]

Law No. 27/2022 enumerates several lawful bases for personal data processing, including consent, contract performance, compliance with legal obligations, protection of vital interests, public interest, and legitimate interests of controllers (Articles 11–12). This multi-tiered approach resonates with comparative frameworks such as the GDPR[29] and Singapore's Personal Data Protection Act (PDPA).[30] Scholarly debates diverge on the primacy of consent versus legitimate interests, like Solove[31] argues that overemphasizing consent risks formalism and user fatigue, while Warren and Brandeis[32] emphasize consent as the moral foundation of privacy, legitimizing individual autonomy in the face of corporate power. Law No. 27/2022

[26]Talia B. Gillis, and Josh Simons. "Explanation< Justification: GDPR and the Perils of Privacy." *Journal of Law & Innovation* 2, no. 1 (2021): 71-99.
[27]Fred H. Cate, "The limits of notice and choice." *IEEE Security & Privacy* 8, no. 2 (2010): 59-62.
[28] Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah. "Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment." *Hasanuddin Law Review* 10, no. 1 (2025): 1-20.
[29]*See* Alan Calder, *EU GDPR: A Pocket Guide*. IT Governance Ltd, 2018.
[30]Warren B. Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform." *Computer Law & Security Review* 29, no. 5 (2013): 554-575.
[31]Daniel J. Solove, "The Limitations of Privacy Rights." *Notre Dame Law Review* 98, no. 3 (2023): 975-1036.
[32]Samuel D. Warren, and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.

attempts a hybrid approach, recognizing consent as central while permitting alternative lawful bases to balance regulatory flexibility with data subject protection.[33]

Nevertheless, the recognition of "legitimate interests" under Article 11 constitutes one of the most contentious aspects of Law No. 27/2022. Unlike consent, which requires an explicit expression of the data subject's will, the concept of legitimate interests is inherently flexible and susceptible to broad interpretation. In practice, digital platforms may invoke this provision to justify extensive data collection, behavioural profiling, targeted advertising, or algorithmic optimization without obtaining explicit consent from users. This risk is particularly significant given Indonesia's evolving institutional framework for data protection, where the absence of a fully independent supervisory authority and detailed implementing regulations may limit effective oversight of controllers' reliance on legitimate interests. Consequently, the provision has the potential to become a regulatory loophole that privileges commercial interests over the privacy rights of data subjects.

A comparative perspective illustrates this regulatory challenge more clearly. Under Article 6(1)(f) of the GDPR, processing based on legitimate interests is not unrestricted but is subject to a rigorous balancing test requiring controllers to demonstrate that their legitimate interests are not overridden by the fundamental rights and freedoms of the data subject. The GDPR further requires transparency, accountability, and documentation of this assessment, while supervisory authorities retain the power to review and challenge controllers' reliance on this legal basis. By contrast, although Law No. 27/2022 adopts the terminology of legitimate interests, it does not prescribe comparable balancing criteria or procedural safeguards to determine when such interests may lawfully outweigh individual privacy rights. The absence of clear implementing parameters creates legal uncertainty and increases the possibility of inconsistent interpretation by data controllers. Consequently, while Law No. 27/2022 represents a significant advancement in Law No. 27/2022, its effectiveness will depend on the development of implementing regulations that establish objective standards for assessing legitimate interests and strengthen institutional oversight to prevent abuse in the digital economy.

Under Articles 12–17, consent in Law No. 27/2022 is defined as a "*freely given, specific, informed, and unambiguous agreement*" to the processing of personal data. This codification aligns with international norms and addresses deficiencies in previous electronic contracting practices, where consent was often embedded within standard form contracts or clickwrap agreements. Scholars such as Bygrave[34] and Kuner[35] highlight the importance of substantive

[33]Edmon Makarim, "Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach." *Data Protection Around the World: Privacy Laws in Action*. The Hague: TMC Asser Press, 2020, pp. 127-164. For various cases, *see also* Nur Azisa, et al. "Additional Criminal Revocation of Access to Online Communication Devices for Perpetrators of Electronic-Based Sexual Violence." *Indonesian Journal of Criminal Law Studies* 10, no. 2 (2025): 451-486; Admiral Admiral, et al. "Indonesia's Online Loan Challenges: What Legal Actions Can Solve the Most Pressing Issues?." *Indonesian Journal of Legal Community Engagement* 8, no. 1 (2025): 275-314.

[34]Lee A. Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements." *Oslo Law Review* 4, no. 2 (2017): 105-120.

[35]Christopher Kuner, " The Internet and the Global Reach of EU Law", In *Marise Cremona and Joanne Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2017): 112-145.

consent, emphasizing that consent must be meaningful, revocable, and contextual, rather than a mere procedural formality. The law further imposes limitations on consent in cases involving vulnerable groups, automated profiling, or sensitive personal data, reflecting an attempt to operationalize fairness and proportionality in data processing.

Law No. 27/2022 establishes extensive rights for data subjects, including the right to access, rectify, erase, object, and restrict processing of their personal data (Articles 19–26). These rights resonate with the "*informational self-determination*" principle articulated by scholars such as Westin[36] and reaffirmed in the GDPR framework. Indonesian regulators have emphasized that these rights are not merely declaratory but must be enforceable, with obligations on controllers to respond within prescribed timelines and provide mechanisms for redress. Critics, however, argue that in practice, asymmetrical bargaining power and lack of technical literacy may limit the ability of users to exercise these rights effectively, as emphasized by Cate & Mayer-Schönberger.[37]

Data controllers and processors are legally required to implement appropriate technical and organizational measures to ensure lawful processing, protect data integrity, and prevent unauthorized access (Articles 13, 14, and 29). This aligns with the principle of accountability, emphasizing proactive governance rather than reactive compliance. Scholarly discourse distinguishes between "*formal compliance*" and "*substantive compliance*",[38] highlighting the risk that firms may meet the letter of the law while undermining the spirit of data protection.

---

[36]Alan F. Westin, "Special Report: Legal Safeguards to Insure Privacy in a Computer Society." *Communications of the ACM* 10, no. 9 (1967): 533-537. *See also* Alan F. Westin, "Social and Political Dimensions of Privacy." *Journal of Social Issues* 59, no. 2 (2003): 431-453. Furthermore, *informational self-determination* is a legal and ethical principle that recognizes an individual's right to control their personal data and to decide when, how, and for what purposes information about themselves is collected, processed, and disclosed. The concept emerged from the 1983 decision of the German Federal Constitutional Court in the Census Act Case, which held that unrestricted data collection and use could endanger human dignity and personal freedom in a modern information society. At its core, informational self-determination is closely linked to personal autonomy, as the ability to make free decisions in social, economic, and political life depends on not being subject to constant surveillance or opaque data practices. Without control over personal information, individuals may feel pressured to conform, limit their expression, or avoid certain activities out of fear that their data will be misused. In the digital era, where personal data is continuously generated through online platforms, electronic transactions, and state and private databases, informational self-determination functions as a safeguard against abuse, profiling, and discrimination. It is reflected in contemporary data protection frameworks, such as the EU's General Data Protection Regulation, which emphasize consent, transparency, purpose limitation, and data subject rights. More broadly, the principle reinforces the idea that personal data is not merely a commodity or technical resource, but an extension of the individual's personality that deserves legal protection to preserve dignity, freedom, and trust in the digital environment. *See* Gerrit Hornung, and Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25, no. 1 (2009): 84-88; Florent Thouvenin,"Informational Self-Determination: A Convincing Rationale for Data Protection Law?." *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law* 12 (2021): 246-256; J. C. Buitelaar, "Post-mortem privacy and informational self-determination." *Ethics and Information Technology* 19, no. 2 (2017): 129-142.

[37]Fred H. Cate, and Viktor Mayer-Schönberger. "Notice and consent in a world of Big Data." *International Data Privacy Law* 3, no. 2 (2013): 67-73.

[38]*See* Kuner, " The Internet and the Global Reach of EU Law"; Solove, "The Limitations of Privacy Rights."

Indonesian regulators have increasingly stressed the importance of integrating data protection by design into digital platforms, though enforcement remains a persistent challenge.

Law No. 27/2022 intersects complexly with traditional doctrines of contractual freedom under KUHPer. While contracts remain the primary vehicle for governing platform-user relationships, consent for personal data processing is now constrained by statutory requirements emphasizing voluntariness and informed choice. Edelman and Stemler[39] and Lessig[40] argue that digital contracts often institutionalize consent as a formalistic tool, enabling platform control rather than protecting users. Law No. 27/2022, therefore, attempts to recalibrate the legal landscape, asserting that contractual consent alone is insufficient to justify data processing when structural asymmetries exist. This tension raises critical socio-legal questions about the enforceability of user rights, the legitimacy of take-it-or-leave-it contracts, and the balance between private autonomy and public interest.

Taken together, Law No. 27/2022 reflects an evolving understanding of consent as a normative and regulatory instrument, rather than merely a contractual formality. By codifying specific requirements for meaningful, informed, and revocable consent, the law engages with broader debates in privacy theory, including Westin's informational self-determination, Warren and Brandeis's moral right to privacy, and Bygrave's socio-technical conception of consent. Nevertheless, scholars caution that without structural reforms in digital contracting practices, these provisions risk remaining aspirational. The Indonesian case thus provides an instructive example of the challenges inherent in aligning traditional contract law, platform governance, and modern data protection norms—a tension that resonates across emerging digital economies in Southeast Asia and beyond.

3.3. Digital Contracts as Instruments of Data Governance

In the Indonesian digital economy, digital contracts function not merely as legal instruments to enforce transactional terms but as governance mechanisms that shape how personal data is collected, processed, and commoditized.[41] Situmeang[42] and Wibisana et.al[43] argue that digital contracts on platforms such as Tokopedia, Gojek, Grab, and Bukalapak operate as socio-technical systems, embedding rules, norms, and power relations in coded form. Rather than simple expressions of mutual consent, these contracts configure data flows, determine user entitlements, and align individual behavior with corporate interests, making them central to the legal and political economy of data in Indonesia.

Standard digital contracts operationalize data processing by specifying the categories of data collected, processing objectives, retention timelines, and arrangements for sharing data

[39]Benjamin Edelman, and Abbey Stemler. "From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces." *Harvard Journal on Legislation* 56, no. 1 (2019): 141-197.
[40]Lawrence Lessig, "Re-crafting a public domain." *Yale Journal of Law and The Humanities* 18 (2006): 56-83
[41]Irsan Rahman, et al. "Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions." *Innovative: Journal of Social Science Research* 4, no. 1 (2024): 4314-4327.
[42]Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber." *Sasi* 27, no. 1 (2021): 38-52.
[43]Muharram Wibisana, Jeane Neltje, and Diana Fitriana. "Perlindungan Hukum Bagi Pelaku Usaha Terhadap Tindakan Pembatalan Pembayaran oleh Konsumen E-Commerce dalam Sistem Cash on Delivery (COD) Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *Krtha Bhayangkara* 17, no. 2 (2023): 437-464.

with third parties. For example, Gojek's terms of service permit the collection of precise geolocation and transactional data for various purposes, including service personalization, analytics, and integration with external partners. Indonesian legal scholars such as Hidayat et.al[44] and Utama[45] highlight that such provisions create private governance architectures, whereby platforms internally regulate personal data processing with minimal public oversight. This aligns with Zuboff's concept of "*surveillance capitalism*,"[46] in which contractual forms enable corporate extraction of behavioral data under the guise of service provision.

Consent clauses embedded in Indonesian platform contracts typically appear within lengthy terms of service and privacy policies, often presented as a single bundled agreement. Tokopedia's 2020 and 2022 privacy policies, for instance, require users to agree to extensive data sharing for analytics and marketing purposes as a condition of service use—a practice critiqued by Indonesian researchers such as Ananta[47] as legally problematic and ethically opaque. These clauses are rarely negotiable; users must accept all terms holistically, eroding the voluntariness of consent. This bundling resonates with global critiques by Edelman[48] and van Dijck[49], who characterize clickwrap architectures as formalistic artifacts that legitimize broad data extraction without substantive user agency.

Despite the requirements of Law No. 27/2022 for transparency and informed consent as articulated in Articles 12–17, Indonesian studies indicate persistent problems in accessibility and comprehension. A 2022 Kominfo digital literacy report found that a significant portion of users do not read or understand terms of service and privacy policies, particularly in rural and lower-income demographics. Rossi[50] and Friedman et.al[51] emphasize that linguistic complexity, legal jargon, and interface design diminish the practical effectiveness of consent as a protective mechanism. From a socio-legal perspective, this gap between legal

[44]Nurul Hidayat, et al. "Penegakan Hukum Terhadap Penyalahgunaan Data Pribadi Pengguna E-Commerce Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Journal of Innovation Research and Knowledge* 5, no. 2 (2025): 1221-1230.

[45]Anugrah Prima Utama, "Provider's Responsibility for Consumer Personal Data in Starter Pack Registration." *Indonesia Private Law Review* 4, no. 1 (2023): 1-8. *See also* Tegar Islami Putra, et al. "Critically Reveal the Dimensions of Damage from Unauthorized Use of Personal Data: Study of Decision Number 78/Pid. Sus/2024/PN. Tng." *The Digest: Journal of Jurisprudence and Legisprudence* 5, no. 2 (2024): 231-262; Tegar Islami Putra, Nurul Fibrianti, and Rizky Andeza Prasetya. "Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)." *Journal of Private and Commercial Law* 9, no. 1 (2025): 72-109; Suraji Suraji, and Ipop Abdi Prabowo. "Harmonizing Privacy Rights Protection in Electronic Transaction with Roscoe Pound's Legal Principle." *Indonesian Journal of Advocacy and Legal Services* 7, no. 1 (2025): 71-94.

[46]Shoshana Zuboff, "Surveillance Capitalism and the Challenge of Collective Action." *New Labor Forum* 28, no. 1 (2019): 10-29.

[47]Magrina Ananta, "Perlindungan Hukum Terhadap Perdagangan Barang Pada Marketplace Perspektif Peraturan Perundang-Undangan di Indonesia". *Dissertation*. Jambi: Universitas Jambi, 2025.

[48]Aaron Benjamin Edelman, "Increasing Lapses in Data Security: The Need for a Common Answer to What Constitutes Standing in a Data Breach Context." *Journal of Law and Policy* 28, no. 1 (2019): 150-194.

[49]Jan Van Dijk, *The Digital Divide*. John Wiley & Sons, 2020.

[50]Arianna Rossi, "Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts." *Dissertation.* Luxembourg: University of Luxembourg, 2019.

[51]Batya Friedman, Peyina Lin, and Jessica K. Miller. "Informed consent by design." *Security and Usability* 2001 (2005): 503-530.

requirements and user experience highlights the limitations of procedural consent in contexts of unequal information and power asymmetry.

The problem of bundled consent—where consent to data processing is inseparable from other contractual obligations—raises profound normative concerns. Prasetyo et.al[52] argue that take-it-or-leave-it contracts distort the voluntariness required under Law No. 27/2022 by presenting users with no feasible alternative if they wish to access essential services. Candraningrat et.al[53] further demonstrate, through qualitative interviews, that users often feel compelled to consent to broad data collection because refusal effectively excludes them from digital participation. This reinforces Solove's critique that formal consent mechanisms may legitimize asymmetrical power dynamics rather than protect individual autonomy.[54]

While many Indonesian platforms have updated privacy policies to nominally align with Law No. 27/2022 consent requirements, substantive compliance remains uneven. For example, Bukalapak's 2023 revisions include explicit provisions on user revocability of consent and purpose limitation.[55] However, these provisions are embedded within dense contractual text that remains inaccessible to many users.[56] Furthermore, Dewi et.al critique such updates as "superficial harmonization," where formal compliance with statutory language does not necessarily translate into practical adherence to substantive consent principles.[57] This distinction between formal legal conformity and substantive realization of rights reflects wider debates in the literature on data protection governance.[58]

Viewed through a socio-legal lens, digital contracts in Indonesia exemplify the broader challenges of aligning contractual freedom with robust data protection. While Law No. 27/2022 articulates meaningful standards for informed and revocable consent, entrenched contracting practices and market power disparities shape how these norms operate in practice. Hayati[59] argue that without addressing structural issues—such as platform dominance, low digital literacy, and asymmetric bargaining power—consent will remain a formalistic device with limited protective effect. These dynamics underscore the importance of integrating

---

[52]Eko Prasetyo, Vallencia Nandya Paramitha, and Fathul Hamdani. "Keabsahan Kontrak Otomatis yang Diproses oleh Artificial Inteligence (AI) dalam Kontrak Bisnis pada Platform Finance Technology (Fintech) di Indonesia." *Lex Journal: Kajian Hukum dan Keadilan* 9, no. 2 (2025): 493-511; Pratama Agus Widodo. "The Role of Indonesian Fatwa Institutions in Responding to Artificial Intelligence Technology." *The Indonesian Journal of Islamic Legal Modernism* 1, no. 1 (2026): 121-150.

[53]Candraningrat Candraningrat, et al. "The Dynamics of Digital Capabilities: Antecedents, Consequences, and Research Agenda." *TEM Journal* 14, no. 3 (2025).

[54]*See* Solove, "The Limitations of Privacy Rights."

[55]*See* PRNewswire, "Bukalapak Enhances Platform's Security and User Comfort", *Online News PR Newswire,* August 29, 2024. Retrieved from https://www.prnewswire.com/news-releases/bukalapak-enhances-platforms-security-and-user-comfort-302234726.html

[56]*See also* Thomas Ericson Hadinata Sihite, Dewi Iryani, and Puguh Aji Hari Setiawan. "Legal Protection of Consumer Personal Data in Electronic Transactions with Legal Certainty." *Ilmu Hukum Prima (IHP)* 8, no. 2 (2025): 8-20; Ario Wendra Wendra, "Study of Raw Contracts in Electronic Contracts in the Digital Era Based on Indonesian Contract Law." *Strata Law Review* 2, no. 1 (2024): 20-50.

[57]Irlina Dewi, et al. "Legality of E-Commerce Transactions: A Comparative Analysis of Islamic Law and Indonesian Civil Law." *Nuansa Akademik: Jurnal Pembangunan Masyarakat* 10, no. 2 (2025): 601-624.

[58]Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements." *See also* Cate, and Mayer-Schönberger, "Notice and consent in a world of Big Data."

[59]Adis Nur Hayati, "Rethinking Consent: Examining the Adequacy of the Concept of Consent in Digital Platform Agreements under Indonesian Civil Code." *Jurnal HAM* 16, no. 2 (2025): 151-164.

doctrinal law, regulatory enforcement, and socio-technical analysis to understand how digital contracts function as instruments of governance, shaping not only legal outcomes but also everyday experiences of privacy and autonomy in the digital economy.

3.4. Legal and Practical Challenges after Law No. 27/2022

In the further context, the reform embodied in Law No. 27/2022 was designed to establish a robust legal framework for personal data governance, yet the enforcement apparatus it created has struggled to cohere into a unified, effective institutional mechanism. Unlike models such as the EU's GDPR regime, where a relatively autonomous supervisory authority (the European Data Protection Board alongside national DPAs) provides a clear locus of enforcement, Indonesia's system disperses authority across multiple entities, chiefly the Personal Data Protection Authority (PDPA)[60] and the Ministry of Communication and Information Technology (*Kominfo*). This duality breeds regulatory ambiguity, while PDPA is theoretically tasked with oversight, Kominfo retains significant substantive and procedural powers that intersect with data protection enforcement, particularly in areas such as data breach reporting and digital content regulation.[61] Indonesian scholars such as Suharto & Kurniawan[62] and Mareati & Awaluddin[63] underscore that overlapping mandates produce institutional friction, impede rapid regulatory response, and create avenues for regulatory capture. Enforcement, when conceived as an exercise of coherent state power to ensure compliance with statutory norms, requires not only legal authority but also institutional clarity. The absence of a clearly demarcated hierarchy of regulatory powers blurs accountability and weakens the capacity to deter non-compliance. This fragmentation, rather than representing a pluralistic strength, diminishes regulatory capacity by diffusing responsibility across multiple agencies that may have divergent institutional cultures and priorities.

In further context, Indonesia's institutional framework for personal data protection also continues to exhibit significant fragmentation, creating uncertainty regarding the allocation of regulatory authority and enforcement responsibilities. Although the Personal Data Protection Law envisages the establishment of a Personal Data Protection Authority (PDPA), the

---

[60]*See* Ali Alibeigi, and Abu Bakar Munir. "A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle." *Journal of Data Protection & Privacy* 5, no. 2 (2022): 119-137; Firsta Rahadatul 'Aisy, Muhammad Azil Maskur, and A. M. Adzkiya 'Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore." *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431-482. *See also* Firdaus Arifin, and Andika Prawira Buana. "Unfair Business Competition in the E-Commerce Ecosystem: Comparison of Indonesian and South Korean Regulations." *Contemporary Issues on Indonesian Social Justice and Legal Reform* 1, no. 1 (2025): 40-57; Fadhel Arjuna Adinda. "Assessing the Economic Impact of Competition Law Enforcement on Market Efficiency in Indonesia". *The Indonesian Journal of Economic Analysis of Law* 1, no. 1 (2026): 31-60.

[61]Vina Himmatus Sholikhah, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah. "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia." *Indonesian Scholars Scientific Summit Taiwan Proceeding* 3 (2021): 54-63.

[62]Budi Suharto, and Arnold Bagas Kurniawan. "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)." *JHP17: Jurnal Hasil Penelitian* 5, no. 2 (2022): 57-61.

[63]Mahisa Mareati, and Agus Awaluddin. "Analisis Hukum Perlindungan Data Pribadi pada Platform E-Commerce di Era Digital: Kajian Yuridis Normatif Terhadap Undang-Undang Nomor 27 Tahun 2022." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 4047-4057.

institutional relationship between the PDPA and the Ministry of Communication and Informatics (Kominfo) remains insufficiently defined. This ambiguity raises several fundamental legal questions concerning which institution ultimately possesses regulatory and supervisory authority, how their respective competencies and jurisdictions are allocated, and whether overlapping mandates may result in ultra vires actions or conflicting administrative decisions. From the perspective of administrative law, unclear institutional boundaries undermine the principle of legal certainty, as regulated entities and data subjects may face uncertainty regarding the competent authority responsible for issuing regulations, conducting investigations, imposing sanctions, or resolving disputes.

The problem extends beyond institutional design to the broader issue of regulatory independence. Unlike GDPR, which requires Member States to establish supervisory authorities that operate with complete independence from political and executive influence, Indonesia has yet to establish a genuinely autonomous data protection authority with clearly guaranteed institutional, financial, and operational independence. The continued concentration of supervisory functions within, or closely linked to, the executive branch creates the risk that enforcement priorities may be influenced by broader governmental objectives, including national digital economy policies, investment promotion, or industrial development. Consequently, regulatory decisions involving major digital platforms or state institutions may be vulnerable to political considerations rather than being guided solely by the protection of fundamental privacy rights and the rule of law.

This institutional arrangement illustrates what may be described as the institutional dependency problem in data protection governance within developing states. Rather than functioning as an independent regulator capable of balancing economic innovation with the protection of individual rights, the supervisory authority remains structurally dependent on executive institutions that simultaneously promote digital transformation and regulate its associated risks. Such dual functions create inherent conflicts of interest and may weaken public confidence in the impartiality of enforcement. Comparative experience under the GDPR demonstrates that effective data protection governance depends not only on comprehensive substantive rules but also on an independent supervisory authority equipped with clearly defined jurisdiction, transparent accountability mechanisms, and adequate enforcement powers. Accordingly, the effectiveness of Law No. 27/2022 will ultimately depend on institutional reforms that eliminate jurisdictional ambiguity, prevent overlapping competencies, and ensure the operational independence necessary to enforce data protection obligations consistently and free from political intervention.

The effectiveness of a data protection regime hinges on the enforcement body's ability to understand, investigate, and sanction complex digital platforms whose architectures continually evolve. The Indonesian enforcement ecosystem faces acute capacity constraints, both in terms of human expertise and technological infrastructure. Digital platforms leverage machine learning techniques, automated profiling, algorithmic personalization, cross-border data flows, and cloud-based ecosystems, all of which create layers of technical complexity that exceed traditional regulatory competencies. Kominfo's own policy forums and public statements acknowledge that enforcement institutions have struggled to build the necessary technical competence to audit platforms' data processing practices, particularly where

algorithmic systems are opaque even to experts within the platforms themselves. This technical asymmetry mirrors broader socio-legal concerns identified by scholars like Zuboff on surveillance capitalism[64], where corporate entities accumulate data and analytical capacity far beyond that of regulatory institutions or data subjects. Law No. 27/2022 grants enforcement authorities powers to investigate, monitor, and sanction, but these powers are rendered less effective if regulators cannot meaningfully interpret or verify compliance with statutory standards, such as lawful bases for processing, proportionality, or data minimization. Regulatory capacity deficits thus transform enforcement from a proactive safeguard into a reactive, almost ad hoc process. Without sustained investment in technical training, collaborative research units, and partnerships with academic institutions, enforcement bodies risk perpetuating a cycle in which technical complexity functions as a shield for non-compliance rather than an impetus for regulatory innovation.

Notwithstanding regulatory ambition, the real test of a legal framework lies in how regulated entities—in this case, digital platforms—translate statutory obligations into operational practices. A pervasive challenge in Indonesia's post-Law No. 27/2022 environment is the existence of compliance gaps, where platforms adopt superficial or cosmetic changes without substantive transformation of data processing practices. This distinction between formal compliance and substantive compliance has been theorized by scholars like Kuner[65] and Solove[66], who caution that legal conformity in text does not necessarily ensure alignment in practice. In the Indonesian context, analyses of revised privacy policies on platforms such as Bukalapak, Gojek, and Tokopedia reveal that updates often consist of declaratory language invoking statutory terms like "revocable consent" or "data subject rights," while the underlying contractual architecture—*a take-it-or-leave-it*, bundled consent regime—remains intact. Dewi et.al characterize these revisions as "surface harmonization," where platforms satisfy the letter of the law in a textual sense but fail to operationalize mechanisms that materially empower users or restrict data exploitation.[67] This phenomenon reflects broader regulatory capture dynamics, where firms adopt minimal compliance postures sufficient to avoid sanctions but insufficient to challenge entrenched business models predicated on extensive data extraction. A key implication is that compliance cannot be equated with capability; platforms may be capable of revising textual documents to signal conformity while simultaneously resisting changes to backend data architectures or consent flows that would reduce their informational advantages.

Law No. 27/2022 emphasizes informed, specific, and freely given consent as a cornerstone for lawful data processing (*see* Articles 12–17). However, the socio-legal reality of

---

[64]Zuboff, "Surveillance Capitalism and the Challenge of Collective Action."
[65]Kuner, " The Internet and the Global Reach of EU Law"
[66]Solove, "The Limitations of Privacy Rights."
[67]Dewi, et.al., "Legality of E-Commerce Transactions: A Comparative Analysis of Islamic Law and Indonesian Civil Law." *See also*, Aisha Rahman, Mr Budi Santoso, and Ms Clara Wijaya. "Safeguarding Privacy in an Interconnected World: Indonesia's Personal Data Protection Law." *International Journal of Social Sciences, Language and Linguistics* 5, no. 3 (2025): 14-18; Gita Venolita Valentina Gea, et al. "Personal Data Protection on International Digital Trade: Harmonizing State Regulations Through a Common Standard." *Veritas et Justitia* 11, no. 1 (2025): 198-225; Engrina Fauzi, et al. "Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty." *Jurnal Ilmiah Ekotrans & Erudisi* 4, no. 1 (2024): 149-157.

consent in Indonesia's digital marketplace often resembles what legal scholars such as Bygrave (2014) and Cate & Mayer-Schönberger[68] describe as procedural consent—a formalistic box-checking mechanism that obscures substantive autonomy. Indonesian digital contracts frequently present consent as an inseparable component of standard terms of service, with privacy clauses embedded deep within dense legal prose. Linguistic complexity, combined with interface design choices that prioritize speed over reflection, limits users' ability to meaningfully engage with the content. Empirical data from Kominfo's digital literacy surveys indicate that a substantial majority of Indonesian users neither read nor comprehend privacy policies before consenting, particularly among lower-income and rural populations. Rosadi et.al[69] observe that even when privacy policies are updated to reflect Law No. 27/2022 language, the accessibility and readability of these documents remain poor, undermining the normative intention of informed consent. This dynamic aligns with broader socio-legal critiques of consent theory, including Fuchs[70], who argues that consent without comprehension and choice is a regulatory simulacrum — a procedural façade that legitimizes power asymmetry while offering little substantive control to data subjects. In practice, therefore, consent retains its formal legal status but loses its normative force as an expression of individual autonomy.

Table 1. Types of Digital Contracts and Their Data Governance Implications

Type of Digital Contract	Common Use in Indonesia	Consent Mechanism	Potential Law No. 27/2022 Concerns	Illustrative Example
Clickwrap	E-commerce platforms, ride-hailing apps	Active "I agree" button	Bundled consent; dense legal language limits informed choice	Tokopedia TOS & privacy policy
Browsewrap	News portals, content streaming	Implied by use of site	Low user awareness; questionable "informed consent"	Kompas.com & streaming portals
Standard Form / Adhesion Contracts	Online banking, fintech, insurance	Signed electronically	Take-it-or-leave-it; high power asymmetry; limited opt-out	OVO, GoPay, Bank Jago digital onboarding

Source: Various sources, edited by Authors

A distinctive challenge in Indonesia's digital contract landscape is the bundling of consent with other contractual terms, producing *take-it-or-leave-it* agreements that force users to accept broad data processing provisions as a condition for platform access. This practice implicates well-established debates in contract theory about freedom of contract and inequality of bargaining power. Traditional contract theory, as articulated by scholars such as

[68]and Mayer-Schönberger Cate, "Notice and consent in a world of Big Data." *See also* Mayer-Schönberger, Viktor. *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt, 2013; Urs Gasser, and Viktor Mayer-Schönberger. *Guardrails: Guiding Human Decisions in the Age of AI*. Princeton University Press, 2024.

[69]Sinta Dewi Rosadi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78-90.

[70]Christian Fuchs, "The digital commons and the digital public sphere: How to advance digital democracy today." *Westminster Papers in Communication and Culture* 16, no. 1 (2021).

Macneil[71], assumes parties possess relatively equal power and understanding; yet in digital marketplaces, this assumption breaks down dramatically. Platforms wield significant market dominance—network effects amplify their strategic leverage—while individual users possess limited alternatives and minimal bargaining power. Prasetyo et.al[72] argue this dynamic effectively neutralizes the voluntariness of consent, turning it into a strategic surrender rather than an exercise of autonomy. Indonesian public interest organizations such as SAFEnet and ICT Watch have documented cases where users report consenting to data processing not out of meaningful choice, but out of necessity, since refusal precludes access to essential digital services. This practice resonates with Edelman's critique of contractual formalism,[73] where consent, stripped of negotiation and meaningful choice, becomes a legal fiction that obscures structural coercion. Law No. 27/2022 intent to ensure meaningful consent, thus collides with entrenched contractual practices that treat personal data as a fungible commodity embedded within broader platform governance regimes.

An effective data protection regime must not only prescribe rights and obligations but also enforce them with credible sanctions that deter non-compliance. Law No. 27/2022 equips regulators with a spectrum of sanctions, including administrative fines, temporary suspension of operations, and even criminal penalties for severe violations. However, Indonesian enforcement authorities have exercised these powers sparingly. Hanafie et.al[74] attributes this caution to a regulatory strategy that prioritizes compliance facilitation and dialogue over punitive measures, reflecting a broader governance culture in which state regulators often adopt a cooperative stance *vis-à-vis* powerful digital incumbents. While collaboration may yield incremental compliance gains, excessive reliance on soft enforcement undermines deterrence and fails to signal that violations carry tangible consequences. In addition, Ayres & Braithwaite[75] argue that effective regulatory regimes balance cooperation with credible sanctions to induce normative internalization among regulated entities. In the Indonesian case, the current emphasis on facilitative measures, when uncoupled from robust deterrence, risks entrenching a regime of weak sanctions that permit ongoing non-compliance with minimal reputational cost. This dynamic is particularly acute in a market environment where regulatory visibility is low, public litigation culture is developing, and platforms calculate that the economic benefits of extensive data exploitation outweigh the potential costs of occasional regulatory scrutiny.

Rights without accessible remedies are rights nominally granted; they are not rights meaningfully protected. Law No. 27/2022 affirms data subjects' rights to access, correct, delete, and seek compensation for improper data processing, but Indonesian procedural

---

[71]Ian R. Macneil, "Relational contract theory: Challenges and queries." *Northwestern University Law Review* 94, no. 3 (2000): 877.

[72]Prasetyo, et.al., "Keabsahan Kontrak Otomatis yang Diproses oleh Artificial Inteligence (AI) dalam Kontrak Bisnis pada Platform Finance Technology (Fintech) di Indonesia."

[73]Edelman, "Increasing Lapses in Data Security: The Need for a Common Answer to What Constitutes Standing in a Data Breach Context."

[74]Nurharsya Khaer Hanafie, et al. "Contemporary Agreement Law Discussing Electronic Agreements in Electronic Media Transactions on The Aspect of Their Legitimacy." *SHS Web of Conferences*. Vol. 149. EDP Sciences, 2022.

[75]Ian Ayres, and John Braithwaite. "Tripartism: Regulatory capture and empowerment." *Law & Social Inquiry* 16, no. 3 (1991): 435-496.

realities complicate the effective exercise of these rights. Judicial routes require users to navigate a complex legal system, bear litigation costs, and meet evidentiary burdens that are particularly onerous in data protection cases. Victims of breaches documented by SAFEnet and LBH Jakarta often struggle to assemble proof of harm, a difficulty compounded by platform control over relevant digital evidence. These concerns raised by Cate & Mayer-Schönberger regarding the access to justice gap inherent in privacy law, even where statutory rights exist, procedural barriers and resource disparities impede their realization.[76] Indonesian CSOs report that many users lack awareness of their rights under Law No. 27/2022, reflecting broader gaps in digital legal literacy. Moreover, alternative dispute mechanisms, such as administrative complaints to PDPA or Kominfo, are relatively untested and lack clear procedural benchmarks for timeliness and transparency. The structural barriers to effective remedy—including information asymmetry, resource constraints, and procedural complexity—thus undermine the Law No. 27/2022 normative promise of enforceable data subject rights.

The judiciary's role in interpreting Law No. 27/2022 and reconciling it with established contract doctrines presents another set of challenges. Indonesian contract law, rooted in the KUHPer and influenced by civil law traditions, emphasizes freedom of contract and the binding nature of agreements entered into by competent parties. However, data protection introduces a set of mandatory norms that constrain contractual freedom where personal data is at issue. This tension evokes debates in comparative law about the limits of contractual autonomy in the face of statutory protections—a theme explored by Davies[77] and Goldsmith & Wu.[78] In the Indonesian context, commentators such as Utomo (2024) caution that without jurisprudence clarifying how courts should prioritize protective data norms over contractual formalism, there is a risk that traditional contract law reasoning could dilute Law No. 27/2022 substantive protections. For example, courts might give primacy to the text of a contract over statutory obligations if they perceive data processing provisions as consensual and voluntarily agreed, even where socio-economic realities suggest otherwise. The judiciary's interpretive approach will therefore be central to shaping how doctrinal tensions between contract law and data protection play out in concrete disputes.

At the theoretical level, the friction between contractual freedom and protective data norms reflects a longstanding debate in legal theory about autonomy, consent, and inequality. Classical contract theory valorizes freedom of contract as an expression of individual autonomy and rational choice; yet critical legal scholars such as Llewellyn[79] and Pound[80] have

[76]*See also* Yuliana Putri, "Digital Surveillance and the Right to Privacy in Indonesia: Between Security and Liberty". *Contemporary Issues on Indonesian Human Rights Law and Policy* 2, no. 4 (2025). https://doi.org/10.65815/85vbtt68; Ratih Damayanti, Duhita Driyah Suprapti, and Rohmat Rohmat. "Judicial Precedents on Privacy Rights: Court Rulings in the Digital Era". *Indonesian Court and Justice Review* 1, no. 4 (2024). https://doi.org/10.65815/j5xmja79.
[77]Paul S. Davies, *JC Smith's the Law of Contract*. Oxford: Oxford University Press, 2018.
[78]Jack Goldsmith, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.
[79]Karl N. Llewellyn, "What Price Contract?. An Essay in Perspective." *The Yale Law Journal* 40, no.5 (1931): 704-751.
[80]Roscoe Pound, "Liberty of Contract." *The Yale Law Journal* 18, no.7 (1909): 454-487.

long recognized that formal freedom masks underlying power disparities. In the digital economy, where platforms exercise significant informational and economic power, this tension becomes particularly acute. Prasetyo et.al[81] argue that data protection norms should function akin to consumer protection doctrines, imposing mandatory limitations on contractual terms that exploit informational advantages. Such an approach resonates with the "relational contract" theory, which emphasizes context, power, and fairness over abstract autonomy. Law No. 27/2022 mandatory consent requirements and data subject rights can be seen as an attempt to recalibrate the normative balance, but without doctrinal frameworks that fully integrate protective norms into contract interpretation, the promise of normative recalibration remains partially unfulfilled.

The global nature of digital platforms means that personal data often traverses national borders, implicating multiple legal regimes and enforcement authorities. Indonesian platforms frequently host data in foreign servers or utilize global cloud services, raising complex questions about jurisdiction, applicable standards, and enforcement reach. Law No. 27/2022 contains provisions suggesting extraterritorial application where data processing affects Indonesian data subjects, but enforcement in cross-border contexts remains untested. The challenges here align with broader international debates about data sovereignty and regulatory fragmentation, as identified in ASEAN comparative studies. Divergent standards across jurisdictions—for example, between Indonesia, Singapore, and the EU—create compliance complexity for multinational platforms. In practice, coordinating enforcement actions across borders requires diplomatic negotiation, mutual legal assistance treaties, and technical cooperation mechanisms, none of which are yet fully developed in the Indonesian context. This fragmentation risks creating regulatory arbitrage opportunities where platforms can structure data flows to minimize exposure to stringent enforcement.

To address ambiguity in statutory language and evolving technological practices, Indonesian regulators have issued soft law instruments, guidelines, and interpretive statements. These are intended to provide clarity on concepts such as lawful bases for processing, data impact assessments, and consent revocability. While soft law can offer valuable interpretive direction, it lacks the binding force of statutory provisions. Rosadi et.al[82] note that reliance on non-binding guidance can produce uncertainty for both regulators and regulated entities, as platforms may selectively adopt interpretations that favor operational convenience rather than substantive protection. The tension between flexibility and legal certainty is well documented in administrative law theory: too rigid a regime stifles innovation, yet too loose a regime undermines predictability. Indonesian data governance currently navigates this tension without a mature jurisprudential foundation to anchor soft law in binding interpretive norms. As a result, compliance uncertainty persists, particularly for emerging digital service providers unfamiliar with data protection expectations.

[81] *See* Prasetyo, et.al., "Keabsahan Kontrak Otomatis yang Diproses oleh Artificial Inteligence (AI) dalam Kontrak Bisnis pada Platform Finance Technology (Fintech) di Indonesia."
[82] Rosadi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?."

3.5. Comparative and Regional Reflections

Law No. 27/2022 emerges not in isolation but within a dynamic ASEAN digital ecosystem characterized by growing interdependence, cross-border platform activity, and regional integration initiatives such as the ASEAN Digital Masterplan 2025.[83] While Indonesia represents a late but comprehensive entrant into the personal data protection space, neighboring ASEAN jurisdictions have pursued diverse regulatory models, reflecting differences in institutional capacity, legal tradition, and economic priorities. Understanding Indonesia's regulatory approach in this regional context illuminates both its comparative strengths and persistent challenges, particularly regarding the operationalization of digital contracts, enforcement of consent norms, and harmonization of cross-border data flows. By situating Indonesia within ASEAN, we can evaluate how regional convergence, or lack thereof, shapes both normative and practical outcomes in digital governance.

Singapore's Personal Data Protection Act (PDPA) 2012, supplemented by advisory guidelines and codes of practice, represents a pragmatic approach that emphasizes proportionality and sector-specific flexibility. Enforcement relies on the Personal Data Protection Commission (PDPC), which adopts a "*facilitative yet sanction-backed*" model, balancing compliance promotion with credible deterrence. Compared to Indonesia, Singapore has developed clearer procedural mechanisms for investigating breaches, providing guidance on consent language, and facilitating dispute resolution. Kuner[84] highlight Singapore's hybrid approach as a model of adaptive regulatory governance, integrating both administrative oversight and soft law instruments. While Indonesia's PDP Law contains similar provisions for consent and user rights, its enforcement architecture remains fragmented, raising questions about the comparative efficiency of multi-agency oversight versus centralized oversight as exemplified by Singapore.

Malaysia's Personal Data Protection Act 2010 (PDPA) emphasizes the primacy of consent and obligations of data users, similar in principle to Indonesia's law. However, Malaysia has faced longstanding challenges with enforcement, including limited awareness among SMEs and reliance on self-regulation.[85] Regional scholars, including Song and Tan[86], note that Malaysia's experience demonstrates the persistent gap between statutory design and operational compliance, especially in terms of informed consent embedded within digital contracts. The Indonesian context mirrors these challenges, but Law No. 27/2022 more explicit articulation of data subject rights and digital contract obligations provides a slightly stronger legal foundation, albeit still constrained by institutional and procedural barriers.

---

[83]*See* ASEAN. *ASEAN Digital Masterplan 2025.* Jakarta: ASEAN Secretariat, 2021. Available online at https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf

[84]*See* Kuner, " The Internet and the Global Reach of EU Law";

[85]*See* Hasventhran Baskaran, et al. "Blockchain and the personal data protection act 2010 (PDPA) in Malaysia." *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*. IEEE, 2020; Edwin Lee Yong Cieh, "Personal data protection and privacy law in Malaysia." *Beyond Data Protection: Strategic Case Studies and Practical Guidance*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 5-29.

[86]Judy Yueh Ling Song, and Esther Tan. "Beyond traditional contracts: the legal recognition and challenges of smart contracts in Malaysia and Singapore." *Journal of Law, Market & Innovation* 3, no.3 (2024): 323-357.

Thailand's Personal Data Protection Act 2019 (PDPA)[87] exemplifies a rigorous alignment with GDPR principles, including robust consent requirements, cross-border data transfer rules, and stringent enforcement mechanisms. Notably, Thailand has adopted explicit guidelines on digital contracting and consent transparency in online services. Comparative analysis reveals that Law No. 27/2022 aligns conceptually with Thailand regarding the emphasis on consent and data subject empowerment. However, Thailand benefits from clearer procedural rules for both administrative complaints and judicial recourse, whereas Indonesia continues to face gaps in accessibility of remedies and public legal literacy. The Thai example underscores the importance of procedural infrastructure in translating statutory rights into practical protections, highlighting areas where Indonesia may focus future regulatory development.[88]

Across ASEAN, a discernible trend is emerging: the convergence of digital governance principles emphasizing consent, transparency, accountability, and cross-border compatibility. Initiatives such as ASEAN's Framework on Personal Data Protection aim to establish baseline standards to facilitate regional digital integration. This harmonization effort has implications for digital contracts, as contractual clauses regarding data processing and consent increasingly need to comply with multiple national frameworks simultaneously. For Indonesian platforms operating regionally, this creates both regulatory complexity and an impetus to adopt best practices. Scholars such as Chander[89] argue that such harmonization encourages platforms to standardize consent mechanisms and privacy disclosures, potentially enhancing user rights but also requiring sophisticated compliance infrastructures.

Effective data protection is essential for ASEAN digital integration, particularly in enabling cross-border e-commerce, fintech, and digital service platforms.[90] Law No. 27/2022, by codifying consent standards and outlining obligations for digital contracts, positions the country to participate meaningfully in regional digital markets. However, the gaps in enforcement, judicial interpretation, and practical operationalization identified earlier may reduce the credibility of Indonesian compliance in cross-border engagements. Regional harmonization efforts, therefore, not only serve normative objectives but also practical economic functions, as data governance becomes a precondition for market access, consumer trust, and cross-border contractual reliability. Comparative analysis suggests that without procedural clarity and institutional strengthening, Indonesia risks lagging behind ASEAN peers in operationalizing these cross-border standards.

---

[87]*See* Thailand. *Thailand Personal Data Protection Act, B.E. 2562*, 2019. Available online at https://mdes.go.th/law/detail/3577-Personal-Data-Protection-Act-B-E--2562--2019-

[88]Chadsada Tungtrakul, Thitirat Thawornsujaritkul, and Thanin Silpcharu. "The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand." *International Journal of Instructional Cases* 8, no.2 (2024): 196-210; Isaravaddee Wongphasukchot, "Online Profiling and Data Protection in Thailand." *Thammasat Business Law Journal* 8 (2018): 47-55.

[89]Anupam Chander, "Is data localization a solution for Schrems II?." *Journal of International Economic Law* 23, no.3 (2020): 771-784.

[90]Yana Chaeru Taufik Ismail, and Arwansyah bin Kirin. "Digital Privacy and Personal Data Protection in Southeast Asia: Challenges and Efforts toward Legal Harmonization." *Justitia Nova* 1, no.1 (2025): 24-34; Sineenat Sermcheep, "Digital Connectivity in ASEAN: Opportunities and Challenges." *Indo-Pacific and ASEAN* (2024): 197-216.

Table 2. Comparative ASEAN Data Protection Approaches

Country	Law & Year	Consent Focus	Enforcement Authority	Cross-Border Data Transfer Rules	Notable Strengths	Key Limitations
Indonesia	Law No. 27/2022	Explicit, informed, revocable	PDPA + Kominfo	Extraterritorial application if affecting Indonesian data subjects	Comprehensive statutory rights; sector-neutral	Fragmented enforcement; limited public literacy
Singapore	PDPA 2012	Emphasis on proportionality	PDPC	Allowed with contractual safeguards	Strong guidance & facilitation; soft law integration	Sector-specific complexity may confuse SMEs
Malaysia	PDPA 2010	Explicit consent; opt-out	Personal Data Protection Commissioner	Allowed with notice & consent	Clear obligations for data users	Limited enforcement capacity; formal compliance often superficial
Thailand	PDPA 2019	GDPR-aligned, robust consent	Personal Data Protection Committee	Strict prior authorization for cross-border transfers	Strong procedural rules; consent clarity	Implementation still developing; digital literacy gap

Source: Various sources, edited by the authors

The comparative and regional perspective illustrates that while Law No. 27/2022 is conceptually aligned with broader ASEAN trends emphasizing consent, transparency, and accountability, practical gaps remain in enforcement, remedy accessibility, and cross-border operationalization. Lessons from Singapore, Malaysia, and Thailand highlight the importance of centralized enforcement structures, procedural clarity, and harmonization with regional frameworks. For ASEAN integration to be meaningful, Indonesia must not only maintain statutory alignment but also strengthen regulatory institutions, build technical expertise, enhance public awareness, and ensure that digital contracts are operationally compliant with both domestic and regional standards.[91]

3.6. Toward an Integrated Regulatory Approach

The Indonesian digital economy continues to expand at unprecedented rates, driven by platform-based services, e-commerce, fintech, and the gig economy. With this expansion, digital contracts have become primary instruments of governance, mediating relationships between users and platforms, and operationalizing the processing of personal data. However, as discussed in prior sections, there is a persistent gap between statutory protection under Law No. 27/2022 and practical enforcement in digital contracting. Current frameworks rely heavily on procedural consent embedded in standard form contracts, which often fails to provide meaningful autonomy to data subjects. This gap is exacerbated by fragmented enforcement institutions and limited public literacy regarding digital rights. A comprehensive regulatory

[91]Julien Chaisse, Georgios Dimitropoulos, and Irma Mosquera. "Law and Digital Transformation in the Indo-Pacific: An International Economic Law Perspective." *The Journal of World Investment & Trade* 1, no. aop (2025): 575-620.

strategy must therefore integrate consent mechanisms, contract law principles, and institutional capacity in a coherent approach that reconciles formal legal rights with operational realities in Indonesia's socio-legal and economic environment.

Consent under Law No. 27/2022 as highlighted on articles 12–17 remains central, but Indonesian scholarship and empirical studies reveal its limitations in practice. For example, research by Dewi et.al[92] and SAFEnet reports indicate that most users accept privacy terms in clickwrap agreements without substantive understanding, reflecting a formalistic consent culture rather than meaningful autonomy.[93] Re-evaluating consent involves both legal and behavioral dimensions: legally, consent should be interpreted in light of good faith and proportionality principles under KUHPer, which can provide doctrinal grounding to limit coercive or bundled contractual clauses. Behaviorally, regulators and platforms should explore design innovations such as layered disclosures, simplified summaries, and interactive consent dashboards, ensuring users can exercise genuine choice. Embedding these principles into law, guidelines, or standard contract clauses would operationalize consent as a normative safeguard, rather than a mere procedural checkbox.

Indonesia's traditional contract doctrine emphasizes freedom of contract and party autonomy. Yet, as Prasetyo et.al[94] argue, freedom of contract cannot operate unbounded in contexts where power asymmetry is structurally entrenched, as in platform-dominated digital markets. To reconcile contract law with Law No. 27/2022 obligations, courts and regulators should adopt an interpretive approach that prioritizes protective norms over formalistic contract clauses, applying doctrines similar to consumer protection law to limit abusive data processing terms. For instance, standard form digital contracts should be scrutinized under principles of unfair terms (Article 1320 KUHPer in tandem with consumer law) and good faith (*itikad baik),* providing a legal lever to ensure that consent clauses and data processing provisions are substantively meaningful. Such harmonization ensures that private contracting does not undermine statutory rights, creating a coherent legal ecosystem where personal data protection and contractual obligations reinforce, rather than conflict with, one another.

Table 3. Enforcement and Compliance Gaps in Indonesia

Challenge Area	Description	Example / Case	Potential Policy Response
Institutional Fragmentation	PDPA + Kominfo share overlapping oversight	Delays in sanctions for Tokopedia data breach (2023 reports)	Clarify agency roles; centralize enforcement authority
Technical Capacity	Regulators lack expertise to audit algorithms & cloud systems	Difficulty monitoring Gojek's data profiling algorithms	Invest in technical teams; collaborate with universities/CSOs
Procedural Consent Issues	Users rarely read TOS; formal consent ≠ informed	SAFEnet survey: 72% of Indonesian users skip privacy policies	Layered disclosure; interactive consent dashboards

[92]Dewi, et al. "Legality of E-Commerce Transactions: A Comparative Analysis of Islamic Law and Indonesian Civil Law."

[93]*See* SAFEnet, "Indonesia's Digital Rights Situation Report 2024 Shows the Legacy of Repression on the Internet", *SAFEnet Report,* February 15, 2025. Retrieved from https://safenet.or.id/2025/03/indonesias-digital-rights-situation-report-2024-shows-the-legacy-of-repression-on-the-internet/

[94]Prasetyo, et.al., "Keabsahan Kontrak Otomatis yang Diproses oleh Artificial Inteligence (AI) dalam Kontrak Bisnis pada Platform Finance Technology (Fintech) di Indonesia."

Challenge Area	Description	Example / Case	Potential Policy Response
Bundled Consent	Take-it-or-leave-it standard clauses	GoPay onboarding combines financial & marketing consent	Mandate separation of essential vs. optional consents
Remedies Access	Litigation cost & evidence asymmetry hinder redress	LBH Jakarta cases on personal data breaches	Administrative complaint channels; fast-track digital dispute resolution

Source: Various sources, edited by the authors

A key mechanism to bridge the gap between law and practice is the introduction of ex ante regulatory instruments. The PDPA, in collaboration with Kominfo, could issue binding guidelines, template consent clauses, or standardized digital contract frameworks that are sector-specific yet aligned with statutory requirements. Such instruments would reduce compliance uncertainty for platforms, provide clear benchmarks for regulators, and ensure users encounter consistent, transparent data processing terms. Indonesia can draw lessons from Thailand's sector-specific guidance and Singapore's PDPC model, adapting these to local socio-economic and linguistic contexts. For instance, guidelines could mandate plain-language summaries of privacy policies, explicit opt-in mechanisms for sensitive data, and provisions for revocation of consent without service denial, operationalizing Law No. 27/2022 rights in practical, enforceable ways.

An integrated regulatory approach requires institutional strengthening, particularly for the PDPA and Kominfo. Regulatory capacity deficits—including limited technical expertise, understaffed enforcement units, and fragmented oversight—constrain the translation of statutory norms into practice. Investment in technical audit teams, digital forensics, and algorithmic compliance monitoring is essential to ensure platforms adhere to contractual and statutory obligations. Moreover, establishing a clear delineation of powers between agencies, coupled with procedural guidance for investigations and sanctions, would reduce institutional overlap and enhance deterrence. Indonesian scholars such as Suharto and Kurniawan[95] argue that capacity building must also extend to public education, enabling data subjects to exercise rights effectively and provide civic oversight of digital contracting practices.

Policy interventions should combine legal reform, regulatory guidance, and socio-technical solutions. First, the law could clarify the mandatory elements of consent, explicitly prohibiting bundled or coercive clauses and requiring layered disclosure for complex processing activities. Second, standard contract clauses, approved by the PDPA, could serve as safe-harbor mechanisms, reducing ambiguity for platforms while protecting user rights. Third, regulators could mandate pre-approval or certification of platform data processing mechanisms, particularly for sensitive sectors like finance, health, and education. Finally, public digital literacy campaigns are essential, ensuring that users understand the implications of digital contracts and their rights under Law No. 27/2022. Together, these measures create a multi-layered regulatory ecosystem, where law, guidance, and socio-technical interventions converge to enforce meaningful data protection.

[95]Suharto, and Kurniawan. "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)."

Table 4. Integrated Regulatory Reform Framework for Personal Data Protection in Indonesia

Structural Problem (Priority)	Regulatory Failure	Proposed Intervention	Expected Normative Impact
High Priority: Standard-form digital contracts provide only formal consent, resulting in consent fatigue and weak user autonomy.	Law No. 27/2022 recognizes consent but provides limited operational guidance on how consent should be obtained in digital interfaces.	Standard Contract Clauses (SCCs) issued by the PDPA, including standardized consent clauses, layered privacy notices, and minimum contractual protections for digital platforms.	Reduces contractual uncertainty, promotes meaningful and informed consent, strengthens user autonomy, and improves regulatory consistency across digital service providers.
High Priority: Preventive oversight of high-risk data processing remains weak, allowing potentially harmful processing before regulatory intervention.	Enforcement is largely reactive, relying on complaints or violations after data processing has occurred.	Ex Ante Certification requiring regulatory assessment of high-risk processing activities before deployment, particularly for fintech, AI, and large digital platforms.	Prevents systemic privacy violations, enhances accountability, increases public trust, and facilitates international data transfers through demonstrable compliance.
Medium Priority: Broad statutory obligations create inconsistent interpretation across industries.	Law No. 27/2022 lacks detailed implementing standards for consent management, data retention, automated profiling, and legitimate interests.	Sector-Specific Guidelines and Soft Law issued by the PDPA for fintech, health, e-commerce, and AI applications.	Closes interpretative gaps without legislative amendment, promotes regulatory certainty, and encourages consistent compliance across sectors.
Medium Priority: Low levels of public awareness reduce the effectiveness of statutory data subject rights.	Legal rights cannot be effectively exercised where individuals lack understanding of privacy risks or available remedies.	Public Digital Literacy Programs through sustained educational campaigns, interactive learning platforms, and partnerships with civil society and educational institutions.	Strengthens informed consent, enhances civic oversight, increases public participation in privacy governance, and improves enforcement through greater awareness of legal rights.
Medium–Long Term: Lengthy and complex privacy policies undermine meaningful consent.	Current disclosure practices satisfy formal legal requirements but fail to ensure user comprehension.	Layered Disclosure and Privacy Dashboards incorporating simplified notices, standardized icons, granular consent controls, and real-time privacy management tools.	Improves transparency, facilitates continuous and revocable consent, reduces information asymmetry, and shifts compliance from formal disclosure to substantive user engagement.
Long-Term Structural Reform: Fragmented institutional governance weakens enforcement and accountability.	The absence of a fully independent supervisory authority creates overlapping jurisdiction and inconsistent regulatory oversight.	Establish an Independent Personal Data Protection Authority with clear statutory powers, financial autonomy, investigative authority, and sanctioning competence.	Enhances legal certainty, eliminates jurisdictional conflicts, strengthens impartial enforcement, and aligns Indonesia's governance framework with international best practices, particularly the GDPR.

Source: Various sources, edited by the authors

Therefore, moving toward an integrated regulatory approach requires recalibrating the balance between contractual freedom and protective norms, operationalizing consent, and embedding enforcement mechanisms into practice. Indonesia's unique socio-legal

environment—characterized by high platform reliance, linguistic and digital literacy diversity, and institutional fragmentation—demands solutions tailored to local realities rather than wholesale adoption of foreign models. An integrated framework combining doctrinal harmonization, ex ante regulatory tools, capacity building, and public engagement offers a pathway to strengthen the substantive protection of personal data while maintaining the flexibility necessary for a vibrant digital economy. Such an approach transforms digital contracts from instruments of mere legal formality into operational vehicles of data governance, user empowerment, and normative coherence, setting a model for ASEAN-level harmonization and regional digital integration.

4. Conclusions

This study has critically examined the intersection of digital contracts and personal data protection in Indonesia following the enactment of Law No. 27/2022. The analysis highlights that while digital contracts are central to operationalizing data processing in platform-based economies, their standardization, bundled consent practices, and asymmetrical power dynamics often undermine the substantive protection of data subjects. The study identifies gaps in institutional enforcement, procedural clarity, and public awareness, revealing that formalistic consent under digital contracts frequently fails to achieve meaningful autonomy. Comparative analysis with ASEAN peers such as Singapore, Malaysia, and Thailand further underscores the importance of harmonizing statutory norms with practical enforcement mechanisms, standard clauses, and user-centered procedural controls. By situating Indonesia within this regional and socio-legal context, the research demonstrates both the potential and the limitations of digital contracts as instruments of data governance and highlights the critical role of an integrated regulatory approach combining doctrinal harmonization, ex ante controls, and civic engagement.

From a scholarly perspective, this paper contributes to law and technology literature by linking contract law principles, personal data protection norms, and platform governance in an emerging digital economy context. It illustrates how socio-legal dynamics, power asymmetry, and regulatory capacity shape the effectiveness of statutory rights, providing a model for understanding similar challenges in other emerging digital economies in Southeast Asia and beyond. Practically, the findings suggest that Indonesia's regulatory framework can be strengthened through standardization of consent clauses, layered disclosure mechanisms, institutional capacity building, and public digital literacy initiatives. Future research could empirically assess the impact of these interventions, explore user behavior in digital contracting, and investigate the harmonization of personal data protection with cross-border digital trade. Overall, the study underscores that robust, context-sensitive governance of digital contracts is essential for balancing innovation, economic growth, and fundamental data protection rights.

5. Acknowledgements

The authors acknowledge the academic collaboration between the Faculty of Law, Universitas Islam Riau (Indonesia); the Faculty of Law, Universitas Negeri Semarang (Indonesia), and Sociedad Civil de Derecho y Políticas Públicas (SOCIPOL), Barcelona (Spain) which made this research possible.

6. Funding (optional)

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

7. References

Adinda, Fadhel Arjuna. "Assessing the Economic Impact of Competition Law Enforcement on Market Efficiency in Indonesia". The Indonesian Journal of Economic Analysis of Law 1, no. 1 (2026): 31-60. https://inleads.id/publications/index.php/IJEAL/article/view/9.

Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." Lex Scientia Law Review 7, no. 2 (2023): 995-1048. https://doi.org/10.15294/lesrev.v7i2.77881

Admiral, Admiral, et al. "Indonesia's Online Loan Challenges: What Legal Actions Can Solve the Most Pressing Issues?." Indonesian Journal of Legal Community Engagement 8, no. 1 (2025): 275-314. https://doi.org/10.15294/jphi.v8i1.21959

Admiral, Admiral, et al. "Unfair Terms in Standard Digital Contracts: A Hidden Threat to Human Rights and Consumer Justice." Yustisia 14, no. 3 (2025): 312-340. https://doi.org/10.20961/yustisia.v14i3.109656

Ajunwa, Ifeoma, and Austin Kamer. "Data Privacy by Contract." Cardozo Law Review 45, no. 5 (2024): 1436-1491. https://doi.org/10.2139/ssrn.5135563

Alamsyah, Fayhan Rafiq, and David Wilson. "The Role of Digital Economy in Promoting Economic Justice: A Case Study of Indonesia's Tech Sector." Indonesian Economic Justice Review 1, no. 4 (2024). https://doi.org/10.65815/z23ttf59

Alibeigi, Ali, and Abu Bakar Munir. "A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle." Journal of Data Protection & Privacy 5, no. 2 (2022): 119-137. https://doi.org/10.69554/yqug8122

Almeyda, Ivan Taffarel, and Endang Prasetyawati. "Consumer protection for the hacking of personal data of Tokopedia marketplace users." Journal Evidence of Law 3, no. 2 (2024): 206-219. https://doi.org/10.59066/jel.v3i2.680

Ananta, Magrina. Perlindungan Hukum Terhadap Perdagangan Barang Pada Marketplace Perspektif Peraturan Perundang-Undangan di Indonesia. Dissertation. Jambi: Universitas Jambi, 2025.

Andriati, Syarifah Lisa, and Dinda Aprilia Batubara. "The Validity of QR-Code Digital Signature in Contract Towards the Evidence Agenda in Civil Court." Mahadi: Indonesia Journal of Law 3, no. 2 (2024): 95-102.

Arifin, Firdaus, and Andika Prawira Buana. "Unfair Business Competition in the E-Commerce Ecosystem: Comparison of Indonesian and South Korean Regulations." Contemporary Issues on Indonesian Social Justice and Legal Reform 1, no. 1 (2025): 40-57.

ASEAN. ASEAN Digital Masterplan 2025. Jakarta: ASEAN Secretariat, 2021. Available online at https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf

Ayres, Ian, and John Braithwaite. "Tripartism: Regulatory capture and empowerment." Law & Social Inquiry 16, no. 3 (1991): 435-496. https://doi.org/10.1111/j.1747-4469.1991.tb00291.x

Azisa, Nur, et al. "Additional Criminal Revocation of Access to Online Communication Devices for Perpetrators of Electronic-Based Sexual Violence." Indonesian Journal of Criminal Law Studies 10, no. 2 (2025): 451-486. https://doi.org/10.15294/ijcls.v10i2.23100

Banakar, Reza, and Max Travers, eds. Theory and Method in Socio-Legal Research. London: Bloomsbury Publishing, 2005.

Barnes, Wayne. "Online Disinhibited Contracts." Pepperdine Law Review 51, no. 2 (2024): 267-324. https://scholarship.law.tamu.edu/facscholar/1971

Baskaran, Hasventhran, et al. "Blockchain and the personal data protection act 2010 (PDPA) in Malaysia." 2020 8th International Conference on Information Technology and Multimedia (ICIMU). IEEE, 2020. https://doi.org/10.1109/icimu49871.2020.9243493

Basukie, Jessica, Yichuan Wang, and Shuyang Li. "Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets." Technological Forecasting and Social Change 161 (2020): 120310. https://doi.org/10.1016/j.techfore.2020.120310

Buitelaar, J. C. "Post-mortem privacy and informational self-determination." Ethics and Information Technology 19, no. 2 (2017): 129-142. https://doi.org/10.1007/s10676-017-9421-9

Burdon, Mark. Digital Data Collection and Information Privacy Law. Vol. 54. Cambridge University Press, 2020.

Bygrave, Lee A. "Data protection by design and by default: deciphering the EU's legislative requirements." Oslo Law Review 4, no. 2 (2017): 105-120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Calder, Alan. EU GDPR: A Pocket Guide. IT Governance Ltd, 2018.

Candraningrat, Candraningrat, et al. "The Dynamics of Digital Capabilities: Antecedents, Consequences, and Research Agenda." TEM Journal 14, no. 3 (2025). https://doi.org/10.18421/tem143-62

Cate, Fred H. "The limits of notice and choice." IEEE Security & Privacy 8, no. 2 (2010): 59-62. https://doi.org/10.1109/msp.2010.84

Cate, Fred H., and Viktor Mayer-Schönberger. "Notice and consent in a world of Big Data." International Data Privacy Law 3, no. 2 (2013): 67-73. https://doi.org/10.1093/idpl/ipt005

Chaisse, Julien, Georgios Dimitropoulos, and Irma Mosquera. "Law and Digital Transformation in the Indo-Pacific: An International Economic Law Perspective." The Journal of World Investment & Trade 1, no. aop (2025): 575-620. https://doi.org/10.1163/22119000-12340376

Chander, Anupam. "Is data localization a solution for Schrems II?." Journal of International Economic Law 23, no.3 (2020): 771-784. https://doi.org/10.1093/jiel/jgaa024

Chik, Warren B. "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform." Computer Law & Security Review 29, no. 5 (2013): 554-575. https://doi.org/10.1016/j.clsr.2013.07.010

Cieh, Edwin Lee Yong. "Personal data protection and privacy law in Malaysia." Beyond Data Protection: Strategic Case Studies and Practical Guidance. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 5-29. https://doi.org/10.1007/978-3-642-33081-0_2

Creutzfeldt, Naomi, Marc Mason, and Kirsten McConnachie. "Socio-Legal Theory and Methods: Introduction." Routledge Handbook of Socio-Legal Theory and Methods. London: Routledge, 2019, pp. 3-8. https://doi.org/10.4324/9780429952814

Damayanti, Ratih, Duhita Driyah Suprapti, and Rohmat Rohmat. "Judicial Precedents on Privacy Rights: Court Rulings in the Digital Era". Indonesian Court and Justice Review 1, no. 4 (2024). https://doi.org/10.65815/j5xmja79.

Davies, Paul S. JC Smith's the Law of Contract. Oxford: Oxford University Press, 2018.

De Lima, Hellen S., Jupryanto Purba, and Diana Napitupulu. "Analisis Hukum Kontrak dalam Sistem Hukum Indonesia: Perlindungan, Wanprestasi, dan Tantangan Era Digital." Jurnal Hukum Sasana 11, no. 1 (2025): 190-204. https://doi.org/10.31599/sasana.v11i1.3966

Dewi, Irlina, et al. "Legality of E-Commerce Transactions: A Comparative Analysis of Islamic Law and Indonesian Civil Law." Nuansa Akademik: Jurnal Pembangunan Masyarakat 10, no. 2 (2025): 601-624. https://doi.org/10.47200/jnajpm.v10i2.3207

Edelman, Aaron Benjamin. "Increasing Lapses in Data Security: The Need for a Common Answer to What Constitutes Standing in a Data Breach Context." Journal of Law and Policy 28, no. 1 (2019): 150-194.

Edelman, Benjamin, and Abbey Stemler. "From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces." Harvard Journal on Legislation 56, no. 1 (2019): 141-197. https://doi.org/10.2139/ssrn.3106383

Faiqy, Muhammad Raihan, et al. "Urgensi Realisasi Peran Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi." Padjadjaran Law Review 10, no. 1 (2022): 142-156. https://doi.org/10.56895/plr.v10i1.838

Fauzi, Engrina, et al. "Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty." Jurnal Ilmiah Ekotrans & Erudisi 4, no. 1 (2024): 149-157. https://doi.org/10.69989/5f8ff494

Fauzy, Elfian, and Annisa Hafizhah. "Legal analysis of user personal data leak cases at tokopedia." Mahadi: Indonesia Journal of Law 2, no. 1 (2023): 41-52. https://doi.org/10.32734/mah.v2i1.11243

Friedman, Batya, Peyina Lin, and Jessica K. Miller. "Informed consent by design." Security and Usability 2001 (2005): 503-530.

Fuchs, Christian. "The digital commons and the digital public sphere: How to advance digital democracy today." Westminster Papers in Communication and Culture 16, no. 1 (2021). https://doi.org/10.16997/wpcc.917

Gasser, Urs, and Viktor Mayer-Schönberger. Guardrails: Guiding Human Decisions in the Age of AI. Princeton University Press, 2024. https://doi.org/10.1515/9780691256351

Gea, Gita Venolita Valentina, et al. "Personal Data Protection on International Digital Trade: Harmonizing State Regulations Through a Common Standard." Veritas et Justitia 11, no. 1 (2025): 198-225. https://doi.org/10.25123/zbea9p38

Gillis, Talia B., and Josh Simons. "Explanation< Justification: GDPR and the Perils of Privacy." Journal of Law & Innovation 2, no. 1 (2021): 71-99. https://doi.org/10.2139/ssrn.3374668

Goldsmith, Jack, and Tim Wu. Who Controls the Internet?: Illusions of a Borderless World. Oxford: Oxford University Press, 2006. https://doi.org/10.1093/oso/9780195152661.001.0001

Guarín Duque, Gustavo, and Julián David Zuluaga Torres. "Enhancing E-commerce through blockchain (DLTs): the regulatory paradox for digital governance." Global Jurist 20, no. 2 (2020): 20190049. https://doi.org/10.1515/gj-2019-0049

Hamzah, Rosyidi, et al. "Imperfect Information of Bankers Clause in Credit Agreements in Banking Institutions: Further Legal Impact." Lex Scientia Law Review 7, no. 2 (2023): 529-568. https://doi.org/10.15294/lesrev.v7i2.76529

Hanafie, Nurharsya Khaer, et al. "Contemporary Agreement Law Discussing Electronic Agreements in Electronic Media Transactions on The Aspect of Their Legitimacy." SHS Web of Conferences. Vol. 149. EDP Sciences, 2022. https://doi.org/10.1051/shsconf/202214903006

Hartati, Sawitri Yuli, Emelia Kontesa, and Agri Baskara. "Sharia fintech in the digital age: Human Rights in Sharia Fintech Through Criminal Law Safeguards." Indonesian Journal of Criminal Law Studies 8, no. 2 (2023): 289-314. https://doi.org/10.15294/ijcls.v8i2.48678

Hayati, Adis Nur. "Rethinking Consent: Examining the Adequacy of the Concept of Consent in Digital Platform Agreements under Indonesian Civil Code." Jurnal HAM 16, no. 2 (2025): 151-164. https://doi.org/10.30641/ham.2025.16.151-164

Hidayat, Nurul, et al. "Penegakan Hukum Terhadap Penyalahgunaan Data Pribadi Pengguna E-Commerce Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." Journal of Innovation Research and Knowledge 5, no. 2 (2025): 1221-1230. https://doi.org/10.53625/jirk.v5i2.10597

Hornung, Gerrit, and Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." Computer Law & Security Review 25, no. 1 (2009): 84-88. https://doi.org/10.1016/j.clsr.2008.11.002

Iman, Nofie. "The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms." International Journal of Law and Management 66, no. 6 (2024): 774-791. https://doi.org/10.1108/ijlma-12-2022-0258

Irmawan, Wahyu Nandang, et al. "Human Rights in the Digital Age: The Indonesian Judiciary's Response to Internet Censorship and Privacy Laws." Indonesian Court and Justice Review 2, no. 3 (2025). https://doi.org/10.65815/sxen5f47

Ismail, Yana Chaeru Taufik, and Arwansyah bin Kirin. "Digital Privacy and Personal Data Protection in Southeast Asia: Challenges and Efforts toward Legal Harmonization." Justitia Nova 1, no.1 (2025): 24-34.

Judijanto, Loso, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." The Easta Journal Law and Human Rights 3, no. 1 (2024): 20-29. https://doi.org/10.58812/eslhr.v3i01.351

Jurriëns, Edwin, and Ross Tapsell. "Challenges and opportunities of the digital 'revolution' in Indonesia." Digital Indonesia: Connectivity and Divergence 2020 (2017): 275-288. https://doi.org/10.4000/archipel.1804

Kenney, Martin, and John Zysman. "The Rise of the Platform Economy." Issues in Science and Technology 32, no. 3 (2016): 61-69.

Kuner, Christopher. " The Internet and the Global Reach of EU Law", In Marise Cremona and Joanne Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (2017): 112-145. https://doi.org/10.1093/oso/9780198842170.001.0001

Lessig, Lawrence. "Re-crafting a public domain." Yale Journal of Law and The Humanities 18 (2006): 56-83

Lestari, Anggia Putri, Syahla Amany Fatiha, and Sylvia Octa Putri. "E-Commerce in Indonesia's Economic Transformation and Its Influence on Global Trade." International Journal of Computer in Law & Political Science 4 (2024): 10-23.

Llewellyn, Karl N. "What Price Contract?. An Essay in Perspective." The Yale Law Journal 40, no.5 (1931): 704-751. https://doi.org/10.2307/790659

Lupton, Deborah. "Personal data practices in the age of lively data." Digital Sociologies. Policy Press, 2017, pp. 339-354. https://doi.org/10.2307/j.ctt1t89cfr.27

Macneil, Ian R. "Relational contract theory: Challenges and queries." Northwestern University Law Review 94, no. 3 (2000): 877.

Makarim, Edmon. "Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach." In Data Protection Around the World: Privacy Laws in Action. The Hague: TMC Asser Press, 2020, pp. 127-164. https://doi.org/10.1007/978-94-6265-407-5_6

Manggala, Adi Putra, et al. "Legal Review of the Implementation of Electronic Contracts and Protection of Parties in Digital Transactions in Indonesia." International Journal of Service Science, Management, Engineering, and Technology 8, no. 1 (2025): 1-8.

Mareati, Mahisa, and Agus Awaluddin. "Analisis Hukum Perlindungan Data Pribadi pada Platform E-Commerce di Era Digital: Kajian Yuridis Normatif Terhadap Undang-Undang Nomor 27 Tahun 2022." Al-Zayn: Jurnal Ilmu Sosial & Hukum 4, no. 1 (2026): 4047-4057. https://doi.org/10.31289/juncto.v6i2.5443

Maulida, One, and Hari Utomo. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan atas kebocoran data pribadi pengguna dalam perspektif hukum pidana." Indonesian Journal of Law and Justice 1, no. 2 (2023): 1-9. https://doi.org/10.47134/ijlj.v1i2.2011

Mayer-Schönberger, Viktor. Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt, 2013. https://doi.org/10.3359/oz1314047

Möslein, Florian. "Digitized terms: the regulation of standard contract terms in the digital age." European Review of Contract Law 19, no. 4 (2023): 300-320. https://doi.org/10.1515/ercl-2023-2019

Ortino, Matteo. "The Functions of Law and of Digital Platforms in the Payment System." European Business Law Review 33, no. 7 (2022): 1083-1107. https://doi.org/10.54648/eulr2022047

Pamungkas, Bambang Adji. "Feminist Legal Critique of Child Marriage Dispensation Practices in Indonesian Religious Courts." The Indonesian Journal of Feminist Legal Studies 1, no. 1 (2026): 31-60. https://inleads.id/publications/index.php/IJFLS/article/view/2.

Perdana, Muhammad Rizky Aji, Rizki Tri Anugrah Bhakti, and Dwi Afni Maileni. "Validity of Electronic Signatures in Digital Agreements: An Analysis of the Application of the

Intellectual Property Law and the Civil Code in E-Commerce Transactions." Jurnal Mahkamah: Kajian Ilmu Hukum dan Hukum Islam (2025): 565-578. https://doi.org/10.25217/jm.v10i2.7158

Pound, Roscoe. "Liberty of Contract." The Yale Law Journal 18, no.7 (1909): 454-487. https://doi.org/10.2307/785551

Prasetyo, Eko, Vallencia Nandya Paramitha, and Fathul Hamdani. "Keabsahan Kontrak Otomatis yang Diproses oleh Artificial Inteligence (AI) dalam Kontrak Bisnis pada Platform Finance Technology (Fintech) di Indonesia." Lex Journal: Kajian Hukum dan Keadilan 9, no. 2 (2025): 493-511. https://doi.org/10.25139/lex.v9i2.11018

Pratama Agus Widodo. "The Role of Indonesian Fatwa Institutions in Responding to Artificial Intelligence Technology." The Indonesian Journal of Islamic Legal Modernism 1, no. 1 (2026): 121-150. https://inleads.id/publications/index.php/IJILM/article/view/24.

Priyono, Ery Agus, Budiharto Budiharto, and Asri Hayyunniarizka Wulandari. "Regulations for E-Commerce Agreement According to ICT Act and Title III of Indonesian Civil Code." Diponegoro Law Review 4, no. 1 (2019): 76-88. https://doi.org/10.14710/dilrev.4.1.2019.76-88

PRNewswire, "Bukalapak Enhances Platform's Security and User Comfort", Online News PR Newswire, August 29, 2024. Retrieved from https://www.prnewswire.com/news-releases/bukalapak-enhances-platforms-security-and-user-comfort-302234726.html

Putra, Tegar Islami, et al. "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study." Unnes Law Journal 10, no. 2 (2024): 223-254.

Putra, Tegar Islami, et al. "Critically Reveal the Dimensions of Damage from Unauthorized Use of Personal Data: Study of Decision Number 78/Pid. Sus/2024/PN. Tng." The Digest: Journal of Jurisprudence and Legisprudence 5, no. 2 (2024): 231-262. https://doi.org/10.15294/digest.v5i2.19941

Putra, Tegar Islami, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis. "Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection." The Indonesian Journal of International Clinical Legal Education 7, no. 2 (2025): 203-234. https://doi.org/10.15294/iccle.v7i2.21049

Putra, Tegar Islami, Nurul Fibrianti, and Rizky Andeza Prasetya. "Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)." Journal of Private and Commercial Law 9, no. 1 (2025): 72-109. https://doi.org/10.15294/jpcl.v9i1.9370

Putra, Yudha Gaizka, and Adhining Prabawati Rahmahani. "Legal Protection for Victims of Personal Data Leakage (Case Study on Victims of PT Tokopedia in 2020)." International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy 1, no. 1 (2025): 600-612.

Putri, Yuliana. "Digital Surveillance and the Right to Privacy in Indonesia: Between Security and Liberty". Contemporary Issues on Indonesian Human Rights Law and Policy 2, no. 4 (2025). https://doi.org/10.65815/85vbtt68.

Rahadatul 'Aisy, Firsta, Muhammad Azil Maskur, and A. M. Adzkiya 'Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration

Sanctions Enforcement from Ireland, Australia, and Singapore." Journal of Indonesian Legal Studies 10, no. 1 (2025): 431-482. https://doi.org/10.15294/jils.v10i1.13755

Rahman, Aisha, Mr Budi Santoso, and Ms Clara Wijaya. "Safeguarding Privacy in an Interconnected World: Indonesia's Personal Data Protection Law." International Journal of Social Sciences, Language and Linguistics 5, no. 3 (2025): 14-18. https://doi.org/10.55640/ijssll-05-03-03

Rahman, Irsan, et al. "Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions." Innovative: Journal of Social Science Research 4, no. 1 (2024): 4314-4327.

Rivantoro, Ridho, and Dyah Permata Budi Asri. "Tanggung Jawab Hukum Korporasi Atas Kebocoran Data Peserta BPJS Kesehatan Berdasarkan UU No. 27 Tahun 2022: Penelitian." Jurnal Pengabdian Masyarakat dan Riset Pendidikan 4, no. 3 (2026): 16034-16040. https://doi.org/10.31004/jerkin.v4i3.4575

Rosadi, Sinta Dewi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." International Review of Law, Computers & Technology 37, no. 1 (2023): 78-90. https://doi.org/10.1080/13600869.2022.2114660

Rossi, Arianna. "Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts." Dissertation. Luxembourg: University of Luxembourg, 2019.

SAFEnet, "Indonesia's Digital Rights Situation Report 2024 Shows the Legacy of Repression on the Internet", SAFEnet Report, February 15, 2025. Retrieved from https://safenet.or.id/2025/03/indonesias-digital-rights-situation-report-2024-shows-the-legacy-of-repression-on-the-internet/

Salsabila, Ditiya, and Budi Ispriyarso. "Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif di Indonesia." AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam 5, no. 2 (2023): 1343-1354. https://doi.org/10.37680/almanhaj.v5i2.3085

Sermcheep, Sineenat. "Digital Connectivity in ASEAN: Opportunities and Challenges." Indo-Pacific and ASEAN (2024): 197-216. https://doi.org/10.4324/9781003559245-17

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. "Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment." Hasanuddin Law Review 10, no. 1 (2025): 1-20. https://doi.org/10.20956/halrev.v10i1.5016

Sholikhah, Vina Himmatus, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah. "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia." Indonesian Scholars Scientific Summit Taiwan Proceeding 3 (2021): 54-63. https://doi.org/10.52162/3.2021112

Sihite, Thomas Ericson Hadinata, Dewi Iryani, and Puguh Aji Hari Setiawan. "Legal Protection of Consumer Personal Data in Electronic Transactions with Legal Certainty." Ilmu Hukum Prima (IHP) 8, no. 2 (2025): 8-20. https://doi.org/10.34012/jihp.v8i2.7637

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber." Sasi 27, no. 1 (2021): 38-52. https://doi.org/10.47268/sasi.v27i1.394

Solove, Daniel J. "The Limitations of Privacy Rights." Notre Dame Law Review 98, no. 3 (2023): 975-1036. https://scholarship.law.nd.edu/ndlr/vol98/iss3/1

Song, Judy Yueh Ling, and Esther Tan. "Beyond traditional contracts: the legal recognition and challenges of smart contracts in Malaysia and Singapore." Journal of Law, Market & Innovation 3, no.3 (2024): 323-357. https://dx.doi.org/10.13135/2785-7867/11334

Sorisa, Cinda, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." Journal Sains Student Research 2, no. 6 (2024): 586-593. https://doi.org/10.61722/jssr.v2i6.2996

Sucahyanto, Ardhitama. "Digital Society and the Transformation of Community-Based Dispute Resolution in Indonesia." The Indonesian Journal of Sociolegal Development 1, no. 1 (2026): 31-60. https://inleads.id/publications/index.php/IJSLD/article/view/14.

Sugiastuti, Natasya Yunita, and Dian Purnamasari. "Improvement of Substantive Provisions of the Validity of Agreement in the Indonesian Civil Code." Diponegoro Law Review 8, no. 1 (2023): 124-140. https://doi.org/10.14710/dilrev.8.1.2023.124-140

Suharto, Budi, and Arnold Bagas Kurniawan. "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)." JHP17: Jurnal Hasil Penelitian 5, no. 2 (2022): 57-61.

Supeno, Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal. "Personal Data Protection in Review of Legal Theories and Principles." Journal of Law and Legal Reform 6, no. 3 (2025): 1349-1376. https://doi.org/10.15294/jllr.v6i3.10252

Suraji, Suraji, and Ipop Abdi Prabowo. "Harmonizing Privacy Rights Protection in Electronic Transaction with Roscoe Pound's Legal Principle." Indonesian Journal of Advocacy and Legal Services 7, no. 1 (2025): 71-94. https://doi.org/10.15294/ijals.v7i1.22331

Thailand. Thailand Personal Data Protection Act, B.E. 2562, 2019. Available online at https://mdes.go.th/law/detail/3577-Personal-Data-Protection-Act-B-E--2562--2019-

Thouvenin, Florent. "Informational Self-Determination: A Convincing Rationale for Data Protection Law?." JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law 12 (2021): 246-256. https://doi.org/10.2139/ssrn.5282546

Tjipto, Felix Pratama. "Comparative Law Analysis of Consumer Protection Law in E-Commerce Transaction Between Indonesia and United States." UIR Law Review 5, no. 2 (2021): 11-25. https://doi.org/10.25299/uirlrev.2021.vol5(2).7456

Tungtrakul, Chadsada, Thitirat Thawornsujaritkul, and Thanin Silpcharu. "The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand." International Journal of Instructional Cases 8, no.2 (2024): 196-210.

Utama, Anugrah Prima. "Provider's Responsibility for Consumer Personal Data in Starter Pack Registration." Indonesia Private Law Review 4, no. 1 (2023): 1-8. https://doi.org/10.25041/iplr.v4i1.2794

Vallejo, Antonio Orti. "Contractual relationships in collaborative economy platforms." European Review of Private Law 27, no. 5 (2019): 995-1022. https://doi.org/10.54648/erpl2019055

Van Dijk, Jan. The Digital Divide. John Wiley & Sons, 2020.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193-220. https://doi.org/10.2307/1321160

Wendra, Ario Wendra. "Study of Raw Contracts in Electronic Contracts in the Digital Era Based on Indonesian Contract Law." Strata Law Review 2, no. 1 (2024): 20-50. https://doi.org/10.59631/slr.v2i1.103

Westin, Alan F. "Social and Political Dimensions of Privacy." Journal of Social Issues 59, no. 2 (2003): 431-453. https://doi.org/10.1111/1540-4560.00072

Westin, Alan F. "Special Report: Legal Safeguards to Insure Privacy in a Computer Society." Communications of the ACM 10, no. 9 (1967): 533-537.

Wibisana, Muharram, Jeane Neltje, and Diana Fitriana. "Perlindungan Hukum Bagi Pelaku Usaha Terhadap Tindakan Pembatalan Pembayaran oleh Konsumen E-Commerce dalam Sistem Cash on Delivery (COD) Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." Krtha Bhayangkara 17, no. 2 (2023): 437-464. https://doi.org/10.31599/krtha.v17i2.812

Widyawati, Agnes Maria Janni, Mig Irianto Legowo, and Heri Purnomo. "The Validity of Electronic Agreements in the Perspective of Indonesian Civil Law." International Journal of Health, Economics, and Social Sciences (IJHESS) 7, no. 2 (2025): 749-753.

Wongphasukchot, Isaravaddee. "Online Profiling and Data Protection in Thailand." Thammasat Business Law Journal 8 (2018): 47-55.

Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?." Pandecta Research Law Journal 19, no. 2 (2024): 173-202. https://doi.org/10.15294/pandecta.v19i2.13279

Zuboff, Shoshana. "Surveillance Capitalism and the Challenge of Collective Action." New Labor Forum 28, no. 1 (2019): 10-29. https://doi.org/10.1177/1095796018819461