Enigma in Law
https://enigma.or.id/index.php/law

e-ISSN 3026-6068
Vol. 4, No. 2 (2026) · pp. 50–64

ORIGINAL RESEARCH ARTICLE

Bound by Statute, Unpoliced in Practice: Privacy-Notice Non-Compliance and Consent Bundling Across Thirty Indonesian Fintech and Health-Tech Platforms Under Law No. 27/2022

Dian Rahayu[1*], Gayatri Putri[2]

[1] *Department of Management, Enigma Institute, Palembang, Indonesia*
[2] *Department of Library and Informatics Science, Enigma Institute, Palembang, Indonesia*

ARTICLE INFO

Received: November 5, 2026
Revised: November 20, 2026
Accepted: December 8, 2026
Available online: December 19, 2026
Published: December 30, 2026
Keywords Consent bundling; Data protection enforcement; Digital platforms; Law No. 27 of 2022; Symbolic compliance
Correspondence Dian Rahayu · Dian.rahayu@enigma.or.id
ORCID 0009-0009-4653-3148
DOI
https://doi.org/10.61996/law.v4i2.154

ABSTRACT

Background. Law No. 27 of 2022 on Personal Data Protection (UU PDP) became binding on 17 October 2024 under Article 74, yet by November 2026 the Presidential Regulation for its supervisory agency (Articles 58–60) had not been issued and Government Regulation No. 33 of 2026 remained in vacatio legis until 16 January 2027. Cross-sector measurement of compliance is lacking.

Objective. To measure privacy-notice compliance, consent bundling, and the sectoral supervision contrast across thirty licensed Indonesian Fintech (n = 15) and Health-Tech (n = 15) platforms.

Methods. Notices (143,316 words) retrieved in November 2026 were coded on ten statutory indicators (D1–D4 declarative; A1–A6 operational) and four clause pathologies (P1–P4), then interpreted through four classical canons and a five-jurisdiction comparison.

Results. Declarative Notice compliance averaged 0.850 (95% CI 0.800–0.900) against 0.250 (95% CI 0.178–0.322) for Operational Accountability, a gap of +0.600 in all thirty notices (Wilcoxon W = 0, p < 0.0001; paired dz = 2.79). The two scores were not significantly correlated (ρ = 0.280, p = 0.134), and citing UU PDP (43.3%) was not associated with a significant operational difference (p = 0.197). Two-thirds of notices (66.7%) contained consent-bundling clauses within the nullity provisions of Articles 22(5) and 23; 13.3% committed to 72-hour breach notification and a different 13.3% named a reachable Data Protection Officer. Fintech and Health-Tech differed little (0.267 vs. 0.233, p = 0.670).

Conclusion. Notices state far more than they commit to, a pattern compatible with weak enforcement, which motivates five sequenced de lege ferenda institutional reforms.

Copyright © 2026 The Author(s). The authors retain copyright. Published by Enigma Institute.
Access license Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International (CC BY-NC-SA 4.0). Noncommercial sharing and adaptation are permitted with attribution. Adaptations must use the same license.

1. Introduction

Article 28G(1) of the 1945 Constitution (*Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*)[1] supplies the constitutional footing for informational self-determination in Indonesia. It guarantees every person protection of self, family, honour, dignity, and property, as well as security from threat, and it is read together with the guarantee of just legal certainty in Article 28D(1)[2,3]. For almost two decades, statutory concretization of this guarantee stayed scattered. More than thirty sectoral instruments carried it, covering electronic transactions, telecommunications, banking, financial technology, and medical records[4–7]. Law No. 27 of 2022 on Personal Data Protection (*Undang-Undang Pelindungan Data Pribadi*, hereinafter Law No. 27/2022 or UU PDP),[8] enacted on 17 October 2022, was meant to end that fragmentation. Its drafters built an omnibus, comprehensive regime that draws largely, though not identically, on the European Union General Data Protection Regulation (GDPR)[9–11]. Article 74 of Law No. 27/2022 gave all public and private Personal Data Controllers (*Pengendali Data Pribadi*) and Processors a strict two-year statutory adjustment period, which closed on 17 October 2024. Since then, every substantive obligation in the statute has operated as binding positive law. The list is long:

explicit, unbundled consent in Bahasa Indonesia (Articles 20–23); execution of subject rights within 3 × 24 hours (Articles 30, 32(2), 40(2), and 41(1)); retention disclosure and destruction once the retention period ends (Articles 21(1)(d) and 42–45); written data-breach notification, again within 3 × 24 hours (Article 46(1)); mandatory appointment of a Data Protection Officer (*Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi*, DPO) where specific data are processed on a large scale (Articles 53–54); and tiered safeguards for cross-border transfers (Article 56).[12] Administrative fines of up to two percent of annual revenue stand behind all of them (Article 57(2)–(3)).

Over twenty-five months have passed since the Article 74 transition deadline elapsed, and Indonesia's data-protection order now faces a deep institutional paradox. The normative side is clear. Statutory obligations leave no room for doubt, and on 16 July 2026 the executive promulgated Government Regulation (*Peraturan Pemerintah*, PP) No. 33 of 2026 on the Implementing Regulation of Law No. 27 of 2022.[13] This instrument has 12 chapters and 225 articles, among them Article 30(1) on prior lawful basis, Articles 93–95 on data-subject rights and automated decisions, and Articles 114–115 on 3 × 24-hour breach reporting. The institutional side looks different. Articles 58–60 mandate a dedicated Data Protection Supervisory Agency (*Lembaga Pelindungan Data Pribadi*), and Article 58(3) leaves its determination to the President while Article 58(5) delegates further provisions to a Presidential Regulation (*Peraturan Presiden*, Perpres), yet as of November 2026 the agency had still not been constituted[14–17]. During this long supervisory interregnum, administrative enforcement under Article 57 has stayed institutionally dormant.[18] The Ministry of Communication and Digital Affairs (*Kementerian Komunikasi dan Digital*, Komdigi) oversees on an interim basis, and it has reacted mainly to high-profile cyber-incident inquiries under older electronic-system regulations instead of conducting systematic *ex officio* compliance audits.[18,19] Sectoral regulators act in parallel, chiefly the Financial Services Authority (*Otoritas Jasa Keuangan*, OJK) in financial services and the Ministry of Health (*Kementerian Kesehatan*, Kemenkes) in digital healthcare. Their enforcement rests on market-conduct and medical-confidentiality rules tied to sectoral licensing, not on the statutory precision of UU PDP[20,21]. Table 1 sets out the primary domestic and comparative legal instruments governing this field.

Table 1. Primary Indonesian and comparative legal instruments analyzed.

Instrument	Year	Jurisdiction	Key provisions relied upon	Status (Nov 2026)
Undang-Undang Dasar Negara Republik Indonesia Tahun 1945	1945/2002	Indonesia	Art. 28D(1) just legal certainty; Art. 28G(1) personal & informational security; Art. 28H(4)	In force
Kitab Undang-Undang Hukum Perdata (*Burgerlijk Wetboek*)	1847	Indonesia	Art. 1320(4) validity of agreements; Art. 1337 unlawful cause (*sebab terlarang*); Art. 1338(3) good faith	In force
UU No. 8 Tahun 1999 tentang Perlindungan Konsumen	1999	Indonesia	Art. 18(1)(a),(g) prohibited standard clauses; Art. 18(3) automatic nullity (*batal demi hukum*); Art. 52(c) BPSK	In force
UU No. 11 Tahun 2008 jo. UU No. 1 Tahun 2024 (UU ITE) & PP No. 71 Tahun 2019 (PSTE)	2008/2024	Indonesia	Art. 26 UU ITE; Art. 14 PP 71/2019 electronic-system principles (existing rules kept in force by Art. 75 UU PDP insofar as they do not conflict)	In force
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)	2022	Indonesia	Arts. 4(2), 5–13, 20–23, 30, 32(2), 35, 39, 40–46, 53–54, 56–60, 74–75	Binding since 17 Oct 2024; Art. 58(5) Perpres unissued
PP No. 33 Tahun 2026 tentang Pelaksanaan UU No. 27 Tahun 2022	2026	Indonesia	12 Chapters, 225 Articles: Art. 30(1) legal basis; Arts. 93–95 rights; Arts. 114–115 breach; Art. 225 transition	Promulgated 16 Jul 2026; *vacatio legis* to 16 Jan 2027
UU No. 4 Tahun 2023 (P2SK); POJK No. 22/2023; POJK No. 40/2024; POJK No. 27/2024	2023/2024	Indonesia	Financial-sector market-conduct supervision, consumer consent, P2P lending & digital financial assets	Actively enforced by OJK
UU No. 17 Tahun 2023 tentang Kesehatan; PP No. 28/2024; Permenkes No. 24/2022	2022/2024	Indonesia	Art. 177 Law 17/2023 (patients' health secrets); Art. 39(1) Permenkes 24/2022 (25-year medical-record retention)	Enforced by Kemenkes
Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)	2016/2018	European Union	Arts. 6, 7(4) anti-tying, 12–22, 33–34 (72 h breach), 37–39 (DPO), 44–49, 83 (turnover fines)	Actively enforced by DPAs & EDPB
Personal Data Protection Act 2012 (No. 26 of 2012, rev. 2020)	2012/2020	Singapore	ss. 11(3),(5) universal public DPO, 15–15A deemed consent, 26D (72 h breach), 48J (10% local turnover fine)	Actively enforced by PDPC
Personal Data Protection Act 2010 (Act 709), as amended by Act A1727 (2024)	2010/2024	Malaysia	ss. 6–12, new s. 12A (mandatory DPO), s. 12B (72 h breach notice), s. 129 (cross-border transfer; whitelist removed)	Phased go-live Jan–Jun 2025; enforced by Commissioner
Lei Geral de Proteção de Dados (Law No. 13.709/2018); ANPD Res. 4/2023 & 15/2024	2018/2024	Brazil	Arts. 7–11, 8 §4 void generic consent, 41 universal DPO, 48 breach (3 working days), 52–53 (2% revenue fine)	Actively enforced by ANPD

Note. Primary legal instruments are cited in the numbered reference list. UUD = Undang-Undang Dasar; KUHPerdata = Civil Code; UU = Undang-Undang; PP = *Peraturan Pemerintah*; Perpres = *Peraturan Presiden*; PSE = electronic system operator.

1.1 Theoretical framework: decoupling and the consent fiction

When ambitious statutory mandates outrun the enforcement capacity of administrative bodies, sociological institutionalism and empirical privacy research give sharp tools for predicting how firms will behave. Organizational theorists separate two forms of decoupling. In policy-practice decoupling, regulated firms adopt visible, inexpensive symbolic structures that project external legitimacy, while their core operational routines stay shielded from costly change. In means-ends decoupling, internal compliance rituals multiply without delivering any substantive protection[22,23]. Waldman shows that corporate compliance ecosystems routinely turn statutory rights into managerial artifacts of performative documentation, checkboxes, and self-serving templates[24]. Cohen shows how digital platforms draw on private contract law to shield data-extractive architectures from public oversight[25]. Consent adds a structural pathology of its own to this institutional decoupling. Solove[26], Barocas and Nissenbaum[27], Susser[28], and Cate and Mayer-Schönberger[29] establish that notice-and-consent regimes decay into legal fictions once platforms fold authorization for data processing into take-it-or-leave-it access to a service, exploiting cognitive overload and asymmetric choice architecture[30], while hardly anyone reads the policies that frame the choice[31]. Empirical audits of European websites and mobile ecosystems after the GDPR took effect confirm that manipulative interface designs, preselected consent banners, and incomplete transparency disclosures persisted even under active supervisory threat, and persisted in the audits cited[32–35]; a later scan of 31 countries found little evidence that regulator guidance and fines had changed compliance rates[36]. In Indonesia, recent empirical legal scholarship in Enigma in Law has documented comparable compliance gaps in adjacent domains. One study found that 100 percent of audited digital-platform terms of service retain standard clauses rendered *batal demi hukum* (void by law) under Article 18 of the Consumer Protection Law, which the authors attribute to limited administrative oversight[37]. Another found that public-sector integrity rules suffer acute implementation deficits where independent enforcement mechanisms lag[38].

1.2 Research gap, aims, and hypotheses

Doctrinal commentary on Law No. 27/2022 keeps growing, yet Indonesian scholarship remains overwhelmingly normative and descriptive. Earlier studies address how UU PDP aligns conceptually with peer-to-peer lending[39–41], electronic medical records and telemedicine[42,43], and controller awareness[44]. None of them systematically codes live privacy notices after October 2024 to measure statutory compliance at indicator level. None quantifies the divergence between symbolic disclosure and operational accountability, and none tests whether sectoral supervision by OJK makes up for the missing national data-protection authority. Fintech and Health-Tech are the natural testing ground for Law No. 27/2022. Both sectors process specific (sensitive) personal data under Article 4(2), namely personal financial data (Article 4(2)(f)) and health data and medical records (Article 4(2)(a)), and large-scale processing of such data raises exposure to harm and, at the same time, triggers mandatory DPO appointment under Article 53(1)(c).

This study responds to both the measurement gap and the question of institutional enforcement. It aims to measure statutory privacy-notice compliance and prohibited consent bundling across thirty licensed Indonesian Fintech and Health-Tech platforms, to examine the normative and institutional explanations that the observed pattern suggests, and to formulate a sequenced reform roadmap before PP No. 33/2026 begins operating. Three hypotheses are examined. H1 (Symbolic–Operational Decoupling) expects compliance with the low-cost Declarative Notice indicators (D1–D4) to exceed compliance with the high-cost Operational Accountability indicators (A1–A6). H2 (Ceremonial Statutory Citation) asks whether explicit invocation of Law No. 27/2022 (D1) and declarative completeness are associated with operational compliance or consent unbundling, and expects no association to be detectable. H3 (Absence of Large Sectoral Supervisory Substitution) asks whether OJK market-conduct supervision in Fintech is accompanied by an operational compliance advantage over Health-Tech, and expects no large difference. For H2 and H3 the study reports estimates with intervals and the minimum detectable effect, because a non-significant result at n = 15 per group does not establish equivalence.

2. Methods

2.1 Research type

The study is empirical legal research. Its design pairs a quantitative, cross-sector content analysis of binding corporate privacy notices with dogmatic statutory interpretation and a comparative institutional analysis. Selected clauses are not cited anecdotally. The evidentiary core is instead an original dataset of thirty full-text primary privacy notices, coded in a reproducible way, and the doctrinal and comparative methods then serve to explain what that dataset shows and to translate it into institutional reform.

2.2 Legal research approach and interpretive method

The normative analysis runs in two registers. Under *de lege lata*, the governing provisions of Law No. 27/2022 and PP No. 33/2026 are read one after another through the four classical civil-law canons: grammatical, systematic, teleological, and historical. Under *de lege ferenda*, the empirical prevalence estimates and the interpretive diagnosis together support five sequenced institutional reforms. For the comparative part, Zweigert and Kötz's functional-equivalence method is applied to five jurisdictions chosen for their structural and regional relevance. Indonesia is the first. The European Union follows as the normative baseline of UU PDP. Singapore and Malaysia are peer ASEAN digital economies, with active versus newly amended statutory mandates[45–48]. Brazil completes the set, a large civil-law democracy whose *Lei Geral de Proteção de Dados* [LGPD] likewise saw agency formation delayed before administrative fining began under the *Autoridade Nacional de Proteção de Dados* [ANPD][49].

2.3 Coding scheme mapped to Law No. 27 of 2022

Ten binary compliance indicators (1 = compliant; 0 = non-compliant/absent) and four diagnostic pathology indicators (P1–P4, 1 = pathology present) were mapped directly onto Law No. 27/2022 (Table 2). The aim was to test H1–H3 without mistaking generic transparency prose for auditable governance commitments. The Declarative Notice Index (D1–D4, 0–1 scale) rests on four indicators. D1 is explicit citation of Law No. 27/2022 (Article 74 alignment). D2 is enumeration of processing purposes and personal data categories/relevance (Article 21(1)(b)–(c)). D3 is enumeration of at least two data-subject rights (Articles 5–13 and Article 21(1)(g)). D4 is disclosure of third-party sharing alongside security commitments (Articles 21(1), 35, and 39). Six indicators make up the Operational Accountability Index (A1–A6, 0–1 scale). A1 is unbundled valid consent free of Article 22(5) and Article 23 nullity. A2 is a quantified ≤ 3 × 24-hour controller service-level agreement (SLA) for subject access, rectification, or withdrawal halting (Articles 30, 32(2), 40(2), and 41(1)). A3 is a numeric retention period in years/months (Article 21(1)(d) and Articles 42–45). A4 is written ≤ 3 × 24-hour (72-hour or 3-calendar-day) breach notification to subjects (Article 46(1) and, once in force, PP No. 33/2026 Articles 114–115). A5 is a designated DPO or dedicated Data Privacy Office(r) with a populated, reachable contact (Articles 53(1) and 54). A6 is cross-border transfer safeguards or Indonesian localization (Article 56(1)–(4)). For each platform i, the

platform-level decoupling gap is defined as $\Delta_i = (1/4)\ \Sigma_{j=1\ldots4}\ D_{ij} - (1/6)\ \Sigma_{j=1\ldots6}\ A_{ij}$. A1 is deterministically the complement of P1 and P2 ($A_{1i} = 1$ if and only if $P_{1i} = 0$ and $P_{2i} = 0$). P1–P4 therefore serve strictly as diagnostic disaggregations, not as additive index components, and Sensitivity Model S3 re-estimates all tests on a construct-purified five-item Operational Index (A2–A6) that excludes A1.

Table 2. Operational coding scheme: declarative indicators, operational accountability obligations, and clause pathologies.

Code	Indicator / clause category	Statutory basis (Law No. 27/2022)	Operational coding rule (1 = present/compliant; 0 = absent/non-compliant)
D1	Explicit citation of Law No. 27/2022	Art. 74 (transition alignment)	1 if notice explicitly cites UU No. 27 Tahun 2022 (UU PDP); 0 if citing only pre-2022 or generic laws
D2	Data categories & processing purposes	Art. 21(1)(b)–(c)	1 if notice enumerates both personal data categories/relevance and specific processing purposes; 0 otherwise
D3	Data-subject rights enumerated	Arts. 5–13, Art. 21(1)(g)	1 if notice informs users of ≥ 2 statutory rights (access, correction, erasure, or withdrawal); 0 otherwise
D4	Third-party sharing & security statement	Arts. 21(1), 35, 39	1 if notice identifies third-party recipient categories and states technical/operational security safeguards
A1	Unbundled valid consent architecture	Arts. 20(2)(a), 22(1),(5), 23	1 if free of both browse-wrap deemed consent (P1 = 0) and inseparable T&C bundling (P2 = 0); 0 if bundled
A2	Quantified ≤ 3 × 24 h subject-rights SLA	Arts. 30, 32(2), 40(2), 41(1)	1 if controller commits to fulfilling access, correction, or withdrawal halting within ≤ 3 × 24 h (3 days); 0 otherwise
A3	Numeric retention period stated	Art. 21(1)(d), Arts. 42–45	1 if notice specifies ≥ 1 numeric retention period in years/months; 0 if wholly indefinite (S4 tests max ceiling)
A4	Written ≤ 3 × 24 h breach notification	Art. 46(1); PP 33/2026 Arts. 114–115	1 if controller commits to written breach notice to subjects within ≤ 3 × 24 h (72 h / 3 calendar days); 0 otherwise
A5	Designated DPO with reachable contact	Arts. 53(1), 54	1 if notice designates a DPO or Data Privacy Office(r) / privacy@ channel with populated contact details; 0 otherwise
A6	Cross-border transfer safeguard / localization	Art. 56(1)–(4)	1 if notice commits to Indonesian localization or states Art. 56 transfer tiers (adequacy, binding DPA, or transfer consent)
P1	Pathology: Browse-wrap / deemed-by-use	Arts. 20(2)(a), 22(1), 22(5)	1 if visiting, downloading, accessing, or using the platform is declared to constitute data-processing consent
P2	Pathology: Inseparable T&C incorporation	Arts. 21(1), 22(1), 23	1 if Privacy Policy is declared an "inseparable unity" (satu kesatuan tidak terpisahkan) with general T&Cs
P3	Pathology: Unilateral amendment by use	Art. 21(2), Art. 22(4)–(5)	1 if controller reserves unilateral amendment power and deems continued platform use to constitute acceptance
P4	Pathology: Liability exoneration / indemnity	Art. 12(1), Art. 23; PP 33/2026 Art. 65 (once in force)	1 if controller disclaims liability or compels user indemnification for unauthorized access or third-party misuse

Note. Indicators D1–D4 form the Declarative Notice Index (mean of 4 items); indicators A1–A6 form the Operational Accountability Index (mean of 6 items). Diagnostic pathologies P1–P4 record contractual non-compliance and are not summed into A1–A6. SLA = service-level agreement; DPO = Data Protection Officer; T&C = terms and conditions.

2.4 Sample and retrieval

The sample comprised thirty platforms, chosen purposively so that institutional design would be balanced across the two largest consumer markets in Indonesia that handle Article 4(2) specific personal data. One market was Fintech (n = 15), which deals with personal financial data under Article 4(2)(f). The other was Health-Tech (n = 15), which deals with health and medical data under Article 4(2)(a). Each market was stratified symmetrically over six functional sub-sectors (7, 4 and 4 platforms in the three sub-sectors of each market; Table 3). A platform qualified only if it held an active domestic license or registration, from OJK/Bank Indonesia for Fintech or from Kemenkes/Komdigi PSE for Health-Tech, and if it published a complete, server-rendered privacy notice (≥ 500 words and ≥ 10 privacy-term occurrences) that a standard HTTP GET request could retrieve without any authentication wall. Some candidates failed this test. Their privacy URLs either returned client-side JavaScript application shells (< 4 static privacy-term hits; doku.com, bareksa.com, bankjago.com, alodokter.com, and siloamhospitals.com) or redirected to a marketing homepage (kredivo.id). These were excluded *ex ante*, before any legal coding began, and each was replaced by a platform from the same sub-sector stratum. The thirty full-text notices were all retrieved on 16 November 2026, hashed with SHA-256, and archived. Together they total 143,316 words (mean 4,777.2, SD 4,499.0, median 3,366.5, range 894–17,712 words).

Table 3. Composition of the stratified purposive sample (N = 30 platforms, 6 sub-sectors, 2 specific-data sectors).

Sector & primary sectoral supervisor	Sub-sector stratum	n	Sampled platforms (ID & commercial name)	Word-count mean (range)
Fintech (n = 15; OJK under Law 4/2023, POJK 22/2023, POJK 40/2024, POJK 27/2024 & Bank Indonesia)	P2P Lending & BNPL	7	F01 Akulaku Finance, F02 Indodana, F03 JULO, F04 Modalku, F05 AdaKami, F06 Amartha, F07 Kredit Pintar	5,391 (2,350–14,830)

Sector & primary sectoral supervisor	Sub-sector stratum	n	Sampled platforms (ID & commercial name)	Word-count mean (range)
Fintech	Payments & Aggregators	4	F08 OVO, F09 LinkAja, F10 Midtrans, F11 Cermati	6,180 (1,866–12,313)
Fintech	Wealth-Tech & Digital Assets	4	F12 Bibit, F13 Stockbit, F14 Pintu, F15 Triv	2,363 (1,364–3,961)
Health-Tech (n = 15; Ministry of Health under Law 17/2023, PP 28/2024, Permenkes 24/2022 & Komdigi PSE)	Telemedicine & Care	7	H01 Halodoc, H02 KlikDokter, H03 Good Doctor, H04 YesDok, H05 Sirka, H06 Riliv, H07 Klinik Pintar	7,159 (1,833–17,712)
Health-Tech	Pharmacy, Lab & TPA	4	H08 Lifepack, H09 Prodia, H10 Bumame, H11 AdMedika	2,464 (1,454–4,414)
Health-Tech	Digital Hospitals	4	H12 Eka Hospital, H13 RS Pondok Indah, H14 Ciputra Hospital, H15 Mayapada Hospital	2,860 (894–4,570)

Note. Selection was purposive against criteria of specific-data processing (Art. 4(2)(a),(f)), domestic sectoral registration, and retrievability of complete server-rendered public notices on 16 November 2026 (total corpus = 143,316 words; overall mean = 4,777 words). BNPL = buy now, pay later; TPA = third-party administrator.

2.5 Statistical analysis, power bounding, and sensitivity protocol

Exact two-sided 95% Clopper–Pearson binomial confidence intervals accompany the indicator proportions. The sample is purposive, not random, so these intervals express estimation precision under a binomial model and do not describe national population parameters. For sub-index means, we computed 10,000-iteration bootstrap 95% percentile intervals (seed = 20261116), along with the intraclass correlation (ICC) and the design effect (DEFF). The within-platform decoupling hypothesis (H1) was examined with two-sided Wilcoxon signed-rank tests, paired t-tests, and Cohen's paired d_z. For ceremonial citation (H2), we used Spearman's ρ and Mann–Whitney U tests that compare platforms citing the UU PDP (D1 = 1) with those that do not (D1 = 0). We also fitted an OLS regression in which operational safeguard counts (0–6) were modeled on sector, D1, and $\log_{10}$(Word Count), and we checked it with Variance Inflation Factors (VIF) and MacKinnon–White HC3 standard errors. Between-sector contrasts (H3) relied on Mann–Whitney U tests, Kruskal–Wallis H tests over the six sub-sectors, and two-sided Fisher's exact tests, with Holm–Bonferroni multiplicity adjustment applied across D1–A6. With only n = 15 per group, a non-significant result cannot be read as exact equivalence. We therefore report the 95% Welch confidence interval for Δ_{sector} next to the Minimum Detectable Effect (MDE) at 80% power (α = 0.05, two-sided: Cohen's d = 1.06, or 0.224 Operational Index points). Finally, six sensitivity models (S1–S6) probe how stable the results are under lenient DPO coding, D1 exclusion, A1 exclusion, strict retention ceilings, 50/50 domain weighting, and six-fold Leave-One-Subsector-Out (LOSO) jackknifing.

2.6 Reliability and ethics

Full-context reading against the archived Bahasa Indonesia and English texts was used to verify each of the 30 × 14 = 420 cells, whether positive or negative. Corroborating verbatim clauses were logged in the open dataset. All thirty raw texts, their SHA-256 hashes, and the replication scripts are released, so outside readers can verify the work independently. The analysis drew only on publicly posted corporate notices and legislation, and no human subjects were involved (see Declarations).

3. Results

3.1 Overall prevalence and symbolic–operational decoupling

Across the thirty platforms, overall ten-indicator compliance averages 0.490 (SD = 0.152; 95% bootstrap CI 0.437–0.543; equal 50/50 domain-weighted mean 0.550). Aggregate scores, however, conceal an acute structural split between low-cost declarative disclosures and enforceable operational commitments (Table 4, Figure 1, and Figure 2). Confirming H1, the Declarative Notice Index (D1–D4) averages 0.850 (SD = 0.141; 95% CI 0.800–0.900), with universal compliance on rights enumeration (D3 = 100.0%) and third-party/security statements (D4 = 100.0%), 96.7% on data-and-purpose enumeration (D2, omitted only in H15 Mayapada Hospital's 894-word notice), and 43.3% on explicit Law No. 27/2022 citation (D1). Conversely, the Operational Accountability Index (A1–A6) collapses to 0.250 (SD = 0.209; 95% CI 0.178–0.322), representing an average of just 1.50 of 6 mandatory safeguards (median = 1.0). Eight platforms (26.7%: Akulaku Finance, Amartha, Stockbit, Pintu, Good Doctor, Prodia, RS Pondok Indah, and Mayapada Hospital) score 0/6 (0.000) operationally, and none (0/30) achieves 5/6 or 6/6 (peaking at 4/6 in OVO and Ciputra Hospital).

Table 4. Indicator-level compliance prevalence, sectoral breakdown, and exact tests (N = 30).

Code	Statutory compliance indicator / clause pathology	All (N = 30) n (%)	Exact 95% CI (%)	Fintech (n = 15) n (%)	Health-Tech (n = 15) n (%)	Fisher p	Holm p
D1–D4	Declarative Notice Sub-Index (Mean = 0.850, SD = 0.141)	—	[80.0, 90.0]	0.850	0.850	0.906†	—
D1	Explicit citation of Law No. 27/2022 (Art. 74)	13 (43.3%)	[25.5, 62.6]	6 (40.0%)	7 (46.7%)	1.000	1.000
D2	Data categories & purposes enumerated (Art. 21(1)(b)–(c))	29 (96.7%)	[82.8, 99.9]	15 (100.0%)	14 (93.3%)	1.000	1.000
D3	Data-subject rights enumerated (Arts. 5–13, 21(1)(g))	30 (100.0%)	[88.4, 100.0]	15 (100.0%)	15 (100.0%)	1.000	1.000

Code	Statutory compliance indicator / clause pathology	All (N = 30) n (%)	Exact 95% CI (%)	Fintech (n = 15) n (%)	Health-Tech (n = 15) n (%)	Fisher p	Holm p
D4	Third-party sharing & security statement (Arts. 21(1), 35, 39)	30 (100.0%)	[88.4, 100.0]	15 (100.0%)	15 (100.0%)	1.000	1.000
A1–A6	Operational Accountability Sub-Index (Mean = 0.250, SD = 0.209)	—	[17.8, 32.2]	0.267	0.233	0.670†	—
A1	Unbundled valid consent architecture (Arts. 22(1),(5) & 23)	10 (33.3%)	[17.3, 52.8]	7 (46.7%)	3 (20.0%)	0.245	1.000
A2	Quantified ≤ 3 × 24 h subject-rights SLA (Arts. 30, 32(2), 40(2))	5 (16.7%)	[5.6, 34.7]	4 (26.7%)	1 (6.7%)	0.330	1.000
A3	Numeric retention period stated (Art. 21(1)(d), Arts. 42–45)‡	11 (36.7%)	[19.9, 56.1]	5 (33.3%)	6 (40.0%)	1.000	1.000
A4	Written ≤ 3 × 24 h breach notice to subjects (Art. 46(1))	4 (13.3%)	[3.8, 30.7]	2 (13.3%)	2 (13.3%)	1.000	1.000
A5	Designated DPO with reachable contact (Arts. 53(1), 54)	4 (13.3%)	[3.8, 30.7]	2 (13.3%)	2 (13.3%)	1.000	1.000
A6	Cross-border transfer safeguard / localization (Art. 56)	11 (36.7%)	[19.9, 56.1]	4 (26.7%)	7 (46.7%)	0.450	1.000
P1–P4	Diagnostic Clause Pathologies (1 = Defective Clause Present)	—	—	—	—	—	—
P(any)	Any void consent-bundling clause (P1 or P2; Arts. 22(5), 23)	20 (66.7%)	[47.2, 82.7]	8 (53.3%)	12 (80.0%)	0.245	—
P1	Browse-wrap / deemed-by-use consent (Arts. 20(2)(a), 22(1))	19 (63.3%)	[43.9, 80.1]	7 (46.7%)	12 (80.0%)	0.128	—
P2	Inseparable T&C incorporation clause (Arts. 22(1), 23)	8 (26.7%)	[12.3, 45.9]	2 (13.3%)	6 (40.0%)	0.215	—
P3	Unilateral policy amendment by continued use (Art. 21(2))	8 (26.7%)	[12.3, 45.9]	3 (20.0%)	5 (33.3%)	0.682	—
P4	Data-liability exoneration / user indemnity (Art. 12(1))	18 (60.0%)	[40.6, 77.3]	10 (66.7%)	8 (53.3%)	0.710	—

Note. Sub-index 95% intervals are from a 10,000-iteration bootstrap (ICC = −0.009, DEFF = 1.00); indicator intervals are exact Clopper–Pearson binomial limits. †Two-sided Mann–Whitney U test p-value comparing Fintech with Health-Tech sub-index distributions. ‡Among the 11 platforms stating a numeric period under A3, 6 (20.0% of the sample: JULO, AdaKami, Midtrans, Bibit, Klinik Pintar, Bumame) specify only a statutory minimum floor ("*paling singkat*" [at the shortest] or "*setidaknya 5–25 tahun*" [at least 5–25 years]), while only 5 (16.7%: OVO, KlikDokter, Sirka, Lifepack, Ciputra Hospital) establish a bounded maximum deletion ceiling.

The platform-level Decoupling Gap (Δ_i) averages +0.600 (SD = 0.215; 95% CI 0.525–0.675). Every single platform (30/30, 100.0%) falls strictly inside the Symbolic–Operational Decoupling Zone below the line of equal compliance in Figure 3(a) (Wilcoxon W = 0, $p = 1.86 \times 10^{-9}$; paired t = 15.29, $p = 2.03 \times 10^{-15}$; Cohen's paired $d_z = 2.79$). Deficits cluster sharpest on verifiable external commitments: 86.7% (26/30) omit the mandatory ≤ 3 × 24-hour subject breach-notification clock (only Modalku, LinkAja, Klinik Pintar, and Ciputra Hospital comply); 86.7% (26/30) fail to designate a reachable DPO (only Kredit Pintar, OVO, Halodoc, and Sirka comply); 83.3% (25/30) fail the ≤ 3 × 24-hour rights SLA (23/30 state no numeric SLA at all, AdaKami cites 5 working days, and Kredit Pintar imposes a 10-working-day advance notice on the user); and while 36.7% (11/30) state a numeric retention duration, 20.0% (6/30) state only minimum retention periods taken from anti-money-laundering (AML) or medical-record regulations, leaving 83.3% (25/30) without a bounded maximum deletion ceiling under Articles 42–45.

3.2 Ceremonial statutory citation and policy length

Testing H2 finds no statistically significant association between symbolic transparency and operational compliance. Across all thirty notices, the Declarative and Operational indices are not significantly correlated (Spearman ρ = 0.280, p = 0.134); the interval is wide at n = 30, so a moderate positive correlation cannot be excluded. Platforms explicitly citing Law No. 27/2022 (D1 = 1, n = 13) achieve no statistically significant operational gain over non-citers (D1 = 0, n = 17): 0.308 versus 0.206 (Mann–Whitney U = 141.0, p = 0.197; Welch p = 0.202), and still deploy void consent bundling in 61.5% (8/13) versus 70.6% (12/17) of notices (Fisher p = 0.706; Amartha, Pintu, and Prodia cite UU PDP while scoring 0/6 operationally). In multivariate OLS regression predicting operational safeguard counts (Table 5; $R^2 = 0.207$, all VIF ≤ 1.02), neither Fintech sector (b = +0.148, HC3 p = 0.751) nor UU PDP citation (b = +0.618, HC3 p = 0.210) is significant, whereas $\log_{10}$(Word Count) is marginally positive (b = +1.433, classical p = 0.044, HC3 p = 0.052): a tenfold longer privacy policy (from 1,500 to 15,000 words) is associated with only 1.43 more of 6 operational safeguards.

Table 5. Multivariate OLS regression predicting operational accountability safeguard count (0–6 scale, N = 30).

Predictor variable	Coeff. (b)	Classical SE	95% CI (classical)	Classical t (p)	HC3 SE	HC3 p	VIF
Constant (Intercept)	−3.923	2.400	[−8.856, 1.010]	−1.63 (0.114)	2.399	0.114	—
Sector: Fintech (ref: Health-Tech)	+0.148	0.433	[−0.743, 1.039]	0.34 (0.735)	0.462	0.751	1.02

Predictor variable	Coeff. (b)	Classical SE	95% CI (classical)	Classical t (p)	HC3 SE	HC3 p	VIF
Cites Law No. 27/2022 (D1 = 1)	+0.618	0.435	[−0.276, 1.513]	1.42 (0.167)	0.481	0.210	1.00
$\log_{10}$(Policy Word Count)	+1.433	0.676	[0.044, 2.821]	2.12 (0.044)*	0.702	0.052	1.01

Note. R^2 = 0.207, adjusted R^2 = 0.116, F(3, 26) = 2.26 (p = 0.105). *Classical two-sided t test, p < 0.05. HC3 = MacKinnon–White heteroskedasticity-consistent standard errors; VIF = variance inflation factor.

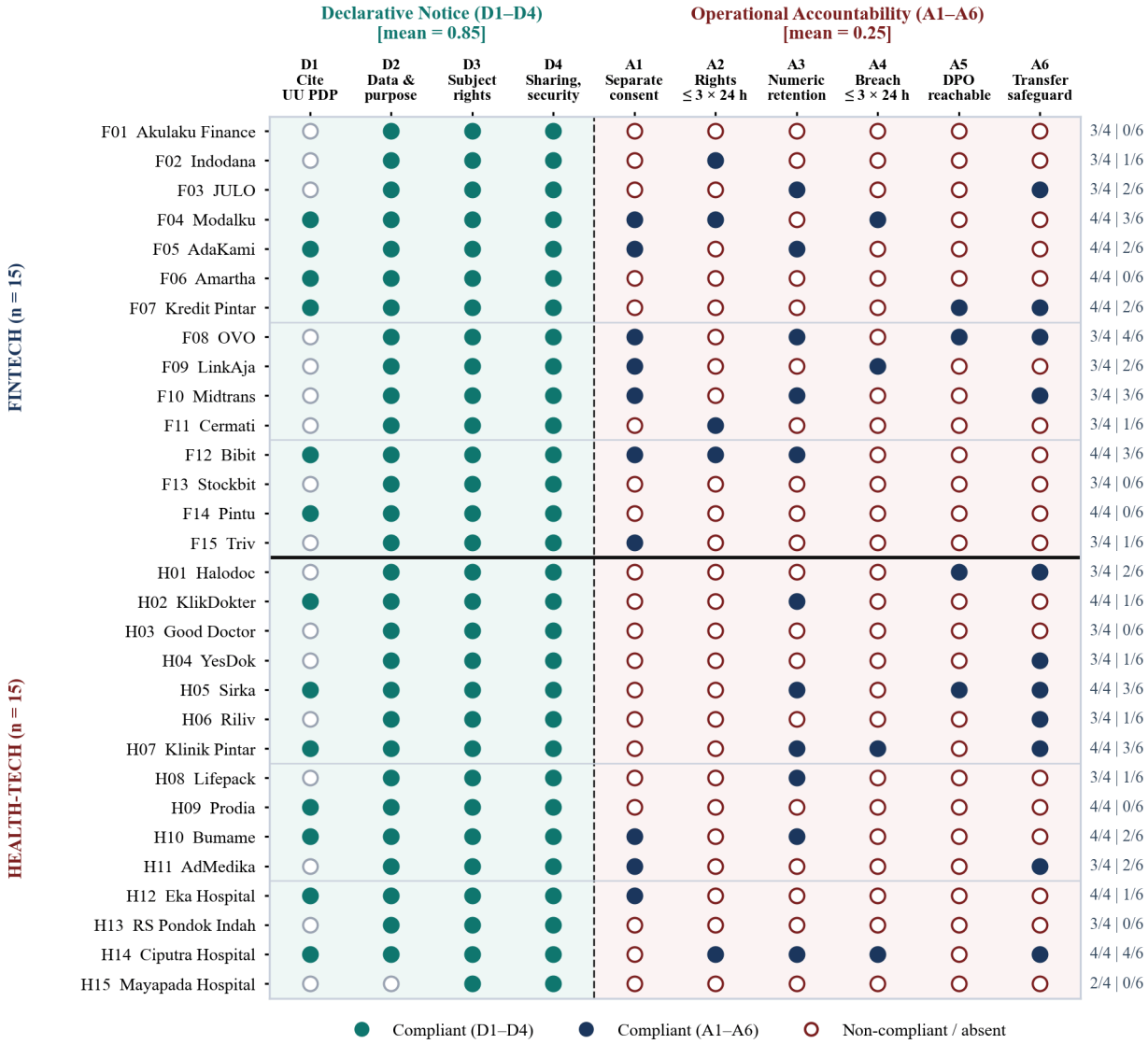

Figure 1. Platform-by-indicator binary compliance matrix across thirty Indonesian Fintech (n = 15) and Health-Tech (n = 15) platforms audited in November 2026 (filled circle = compliant; open circle = non-compliant or absent).

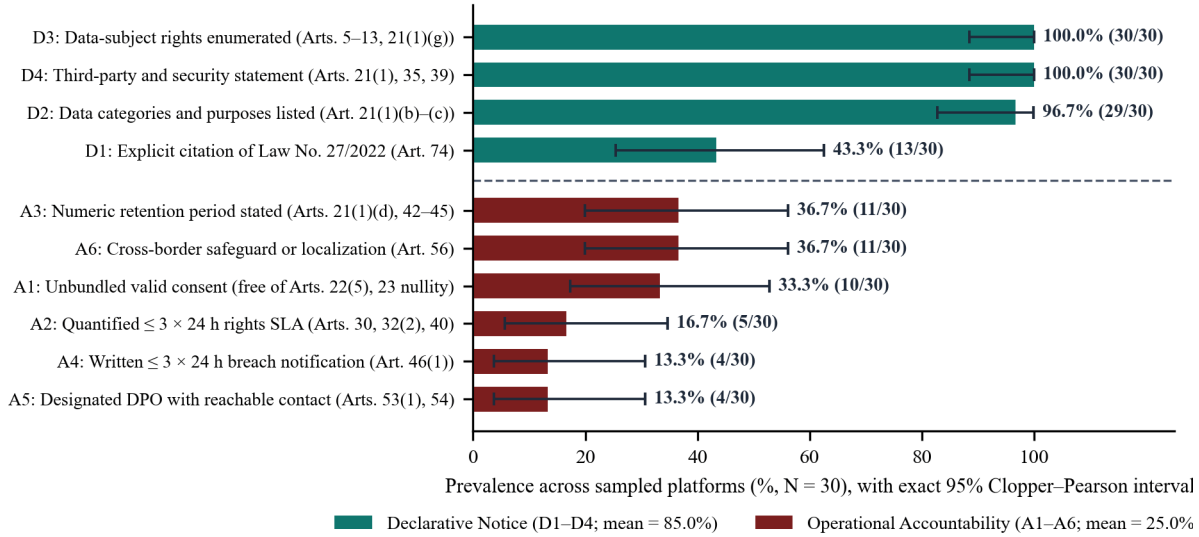

Figure 2. Prevalence of Declarative Notice (D1–D4) versus Operational Accountability (A1–A6) indicators across the thirty platforms, with exact 95% Clopper–Pearson confidence intervals.

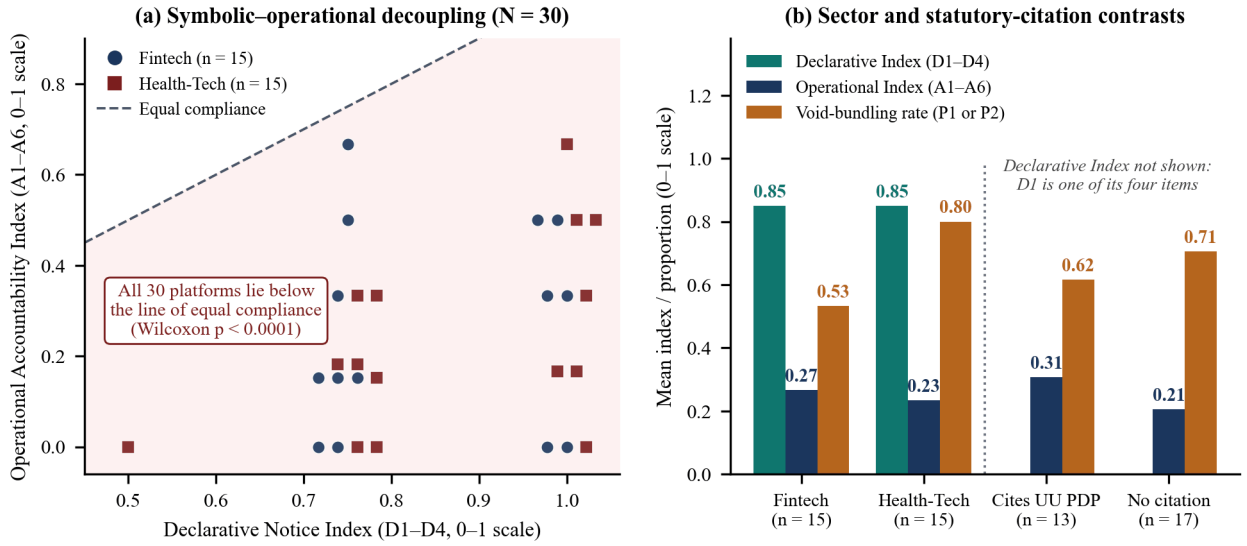

Figure 3. (a) Operational Accountability Index plotted against Declarative Notice Index across all thirty platforms (points sharing identical coordinates are spread slightly so that each is visible). (b) Mean Declarative Index, Operational Index, and void-bundling rate by sector and by UU PDP citation cohort.

3.3 Variation across sectors: Fintech versus Health-Tech

The cross-sectoral comparison is compatible with H3 (Table 6 and Figure 3(b)). Fintech and Health-Tech post identical Declarative means (0.850 vs. 0.850, p = 0.906) and statistically indistinguishable Operational Accountability means: 0.267 (1.60/6) in Fintech versus 0.233 (1.40/6) in Health-Tech (Δ_{sector} = +0.033, 95% Welch CI [−0.125, +0.192]; Mann–Whitney U = 123.0, p = 0.670, r_{rb} = −0.093; sub-sector Kruskal–Wallis H = 3.583, p = 0.611). At n = 15 per group (80%-power MDE = 0.224 index points), the [−0.125, +0.192] interval excludes a sector difference of 0.20 points or more. Sectoral rules shape isolated pockets: Fintech unbundling (A1) is more frequent than in Health-Tech (46.7% vs. 20.0%; Fisher p = 0.245), with the payments and aggregators sub-sector highest (3 of 4 notices unbundled), while numeric retention (A3) is more frequent in Health-Tech (40.0% vs. 33.3%; Fisher p = 1.000), which may reflect the 25-year medical-record rule of Permenkes No. 24/2022 (Article 39(1))[50]; yet on pure UU PDP institutional duties (A4 72-hour breach notice and A5 reachable DPO), both sectors sit at 13.3%.

Table 6. Sectoral and sub-sectoral compliance distributions and non-parametric contrasts (N = 30).

Analytical stratum	n	Declarative Mean (SD)	Operational Mean (SD)	Operational /6 Mean (Med)	Decoupling Gap Mean (SD)	Void Bundling (%)	Exoneration P4 (%)
Sector contrast (p-values: Mann–Whitney U; Fisher's exact for bundling and P4)	30	p = 0.906	p = 0.670	p = 0.670	p = 0.786	p = 0.245	p = 0.710

Analytical stratum	n	Declarative Mean (SD)	Operational Mean (SD)	Operational /6 Mean (Med)	Decoupling Gap Mean (SD)	Void Bundling (%)	Exoneration P4 (%)
Fintech (OJK / BI Regime)	15	0.850 (0.127)	0.267 (0.216)	1.60 (2.0)	+0.583 (0.246)	53.3% (8/15)	66.7% (10/15)
Health-Tech (Kemenkes / PSE Regime)	15	0.850 (0.158)	0.233 (0.207)	1.40 (1.0)	+0.617 (0.186)	80.0% (12/15)	53.3% (8/15)
Sub-sector contrast (Kruskal–Wallis H and p)	30	H = 3.30 (p = 0.654)	H = 3.58 (p = 0.611)	H = 3.58 (p = 0.611)	H = 6.23 (p = 0.284)	—	—
1. P2P Lending & BNPL (Fintech)	7	0.893 (0.134)	0.238 (0.189)	1.43 (1.0)	+0.655 (0.189)	71.4% (5/7)	71.4% (5/7)
2. Payments & Aggregators (Fintech)	4	0.750 (0.000)	0.417 (0.215)	2.50 (2.5)	+0.333 (0.215)	25.0% (1/4)	100.0% (4/4)
3. Wealth-Tech & Digital Assets (Fintech)	4	0.875 (0.144)	0.167 (0.236)	1.00 (0.5)	+0.708 (0.220)	50.0% (2/4)	25.0% (1/4)
4. Telemedicine & Care (Health-Tech)	7	0.857 (0.134)	0.262 (0.189)	1.57 (1.0)	+0.595 (0.148)	100.0% (7/7)	57.1% (4/7)
5. Pharmacy, Lab & TPA (Health-Tech)	4	0.875 (0.144)	0.208 (0.160)	1.25 (1.5)	+0.667 (0.245)	50.0% (2/4)	50.0% (2/4)
6. Digital Hospitals (Health-Tech)	4	0.812 (0.239)	0.208 (0.315)	1.25 (0.5)	+0.604 (0.229)	75.0% (3/4)	50.0% (2/4)

Note. Sector difference on the Operational Index is Δ(sector) = +0.033 (95% Welch CI [−0.125, +0.192]; rank-biserial r = −0.093; 80%-power MDE = 0.224). Kruskal–Wallis rows give H (p). Standard deviations and Kruskal–Wallis statistics were recomputed from Figure 1 (see Change Log).

3.4 Forensic clause pathology and lawful-basis substitution

Close reading of the corpus exposes four pervasive drafting pathologies (Table 7). First, two-thirds of platforms (66.7%, 20/30; 100.0% [7/7] of Telemedicine apps) deploy consent bundling (browse-wrap deemed consent P1, 63.3%; inseparable T&C unity P2, 26.7%; the two overlap) which falls, on its face, within the nullity provisions of Articles 22(5) and 23 (*batal demi hukum*, void by law). Crucially, controllers cannot salvage these clauses by invoking non-consent lawful bases under Article 20(2)(b)–(f) (contractual necessity or legal obligation, reiterated in PP No. 33/2026 Article 30(1)): cross-tabulation reveals that while 17/30 (56.7%) notices mention non-consent bases, 28/30 (93.3%) simultaneously authorize secondary commercial processing (cross-marketing, affiliate promotions, automatic loyalty enrollment such as KlikDokter KPoin, or profiling), and 19 of those 28 platforms (67.9%) sweep that secondary monetization into indivisible browse-wrap or T&C-bundled consent (substitution of the lawful basis).

Second, textual forensics uncover shared boilerplate and uncompleted templates: rival telemedicine apps Halodoc (17,712 words) and YesDok (16,464 words) share near-verbatim identical Bahasa Indonesia paragraphs on chat-history consent, conditional breach notice, and liability disclaimers; Eka Hospital (policy dated 5 May 2026, citing UU PDP) twice directs patients to contact its DPO "pada alamat berikut:" and leaves the email completely blank; and Ciputra Hospital leaves a literal template token Alamat: [ALAMAT] ([ADDRESS]) live in production. Third, Cermati (F11) omits the 3 × 24-hour breach notice under Article 46(1) yet deploys the exact 3 × 24 jam clock in its Force Majeure clause to disclaim cyber-incident liability, while 60.0% (18/30) embed liability exonerations (P4) clashing with Article 12(1) on damages and, once in force, with Article 65 of PP No. 33/2026 (which bars exoneration clauses in privacy notices) and 26.7% (8/30) impose unilateral amendment by continued use (P3), bypassing prior notification under Article 21(2).

Table 7. Representative non-compliant, template-defective, and risk-shifting clauses (November 2026 corpus).

Platform (ID) & sector	Code	Verbatim Bahasa Indonesia clause (abbreviated)	Statutory conflict (Law No. 27/2022)
Amartha (F06), Fintech P2P	P1, P2 (A1=0)	"*Dengan menggunakan Layanan Kami berarti Anda mengakui*... menyetujui seluruh ketentuan... yang adalah satu kesatuan yang tidak terpisahkan dengan Syarat dan Ketentuan Penggunaan." ["By using Our Services you acknowledge … agree to all provisions …, which form one inseparable whole with the Terms and Conditions of Use."]	Deems service use as consent & fuses notice into T&Cs despite citing UU PDP; void *ipso jure* (Arts. 22(1),(5), 23).
Kredit Pintar (F07), Fintech P2P	P1, A2=0	"Dengan mengakses... mengunjungi Platform kami... Anda menyetujui..." / "memberikan pemberitahuan tertulis sekurang-kurangnya sepuluh (10) hari kerja sebelum tanggal penghapusan..." ["By accessing … visiting Our Platform … you agree …" / "give written notice at least ten (10) working days before the date of deletion …"]	Browse-wrap deemed consent (Art. 22(5)) plus inverted 10-working-day user notice burden (Arts. 30, 40(2)).
Cermati (F11), Fintech Aggregator	A4=0, P4	"Dalam hal terjadi Keadaan Memaksa, Kami akan memberitahukan Pengguna *paling lambat* 3 x 24 jam... Kami tidak bertanggung jawab atas... kebocoran Data Pribadi..." ["In the event of Force Majeure, We will notify the User no later than 3 x 24 hours … We are not liable for … leakage of Personal Data …"]	Omits 3 × 24 h breach notice (Art. 46(1)) while using the 3 × 24 h period solely for Force Majeure exoneration (Art. 12(1)).

Platform (ID) & sector	Code	Verbatim Bahasa Indonesia clause (abbreviated)	Statutory conflict (Law No. 27/2022)
Halodoc (H01) & YesDok (H04), Telemed	P1, P2, A4=0	"Dengan menggunakan Platform Kami, Anda dianggap mengakui dan menyetujui bahwa layanan riwayat obrolan... dapat dikumpulkan..." / "...sepanjang di*wajib*kan... memberitahu Anda... secara langsung maupun tidak langsung..." ["By using Our Platform, you are deemed to acknowledge and agree that the chat-history service ... may be collected ..." / "... to the extent required ... to notify you ... directly or indirectly ..."]	Verbatim shared cross-firm template deeming app use to authorize clinical chat collection and hedging 3 × 24 h written breach notice (Arts. 4(2)(a), 22(1), 46(1)).
Eka Hospital (H12), Digital Hospital	D1=1, A5=0	"...menghubungi Kami melalui Pejabat Pelindungan Data Pribadi atau Data Protection Officer kami yang dapat dihubungi melalui surat elektronik atau email pada alamat berikut: [blank]" ["... contact Us through Our Personal Data Protection Officer or Data Protection Officer, who can be reached by electronic mail or e-mail at the following address: [blank]"]	Policy dated 5 May 2026 cites UU PDP and names a DPO twice, yet leaves DPO email completely blank (Arts. 53(1), 54).
Ciputra Hospital (H14), Digital Hospital	D1=1, A5=0	"...silakan menghubungi kami melalui: Ciputra Hospital / Email: info@ciputrahospital.com / Alamat: [ALAMAT]" ["... please contact us through: Ciputra Hospital / E-mail: info@ciputrahospital.com / Address: [ADDRESS]"]	Adopts 3 × 24 h UU PDP clauses yet leaves literal unedited [ALAMAT] ([ADDRESS]) placeholder and omits DPO (Art. 53(1)).

Note. Full Bahasa Indonesia and English contexts are preserved in the replication files named under Data Availability. English renderings in square brackets are the copyeditor's translations of the abbreviated clauses. Coding records *prima facie* textual conflict rather than judicial adjudication.

3.5 Sensitivity and robustness checks

Table 8 summarizes six sensitivity models (S1–S6). Across every specification (crediting unpopulated DPO titles (S1), removing D1 (S2), purifying the Operational Index to A2–A6 without A1 (S3, eliminating any algebraic link to consent bundling), requiring a bounded maximum retention ceiling (S4), applying 50/50 domain weights (S5), and dropping each sub-sector sequentially via six-fold LOSO jackknifing, S6), the decoupling gap remains large (+0.583 to +0.739, all Wilcoxon $p \leq 2.38 \times 10^{-7}$) and sectoral differences remain non-significant (all $p \geq 0.379$).

Table 8. Sensitivity and methodological robustness checks across six alternative specifications (N = 30).

Model	Specification / analytical perturbation	Declarative Mean	Operational Mean	Decoupling Gap (Δ)	Paired Wilcoxon p	Sector Mann–Whitney p
Baseline	Primary 10-indicator specification (D1–D4 vs. A1–A6)	0.850	0.250	+0.600	1.86×10^{-9}	0.670
S1	Lenient DPO rule (crediting unpopulated DPO mentions in H07, H12)	0.850	0.261	+0.589	1.86×10^{-9}	0.848
S2	Pure Art. 21 notice content (excluding D1 statutory citation: D2–D4)	0.989	0.250	+0.739	1.86×10^{-9}	0.670
S3	Construct-purified Operational Index (A2–A6 only, excluding A1)	0.850	0.233	+0.617	1.86×10^{-9}	0.931
S4	Strict maximum retention ceiling (5/30 upper deletion limit on A3)	0.850	0.217	+0.633	1.86×10^{-9}	0.863
S5	Equal 50/50 domain weighting (composite mean = 0.550 vs. 0.490)	0.850	0.250	+0.600	1.86×10^{-9}	0.818
S6	Six-fold Leave-One-Subsector-Out (LOSO) jackknife (n = 23–26)	[0.831, 0.870]	[0.212, 0.278]	[+0.583, +0.641]	$\leq 2.38 \times 10^{-7}$	[0.379, 0.851]

Note. S2 changes only the Declarative Index, so its sector p-value equals the baseline. The S5 sector p-value is for the equal-weighted composite index (Fintech 0.558 vs. Health-Tech 0.542). Model S6 reports [minimum, maximum] bounds across all six sub-sector leave-one-out iterations. S4 and S5 sector p-values were recomputed from Figure 1.

4. Discussion

4.1 Interpreting Law No. 27 of 2022 through four canons

The four classical canons find no ambiguity in the statute that would explain the compliance pattern, which is compatible with an enforcement explanation; other explanations (awareness, cost, waiting for PP No. 33/2026) were not tested. Take the grammatical reading first. Law No. 27/2022 uses the imperative *wajib* (must) again and again. Controllers *wajib* obtain explicit consent separately (Article 22(1)) and notify subjects before amending disclosures (Article 21(2)). They must also honor access, correction, halting, and restriction requests within *paling lambat 3 × 24 jam* (at the latest 3 × 24 hours) (Articles 30, 32(2), 40(2), 41(1)), deliver written breach notices within 3 × 24 jam (Article 46(1)), and appoint a DPO (Article 53(1)). Articles 22(5) and 23 go further: a consent clause that does not conform is void by law (*batal demi hukum*) from the moment it is drafted. The systematic reading comes next. Articles 22(5) and 23 supply specific statutory content for the Civil Code's bar on agreements founded on an unlawful cause (*sebab yang terlarang*, KUHPerdata Articles 1320(4) and 1337)[51], and they run parallel to Article 18(3) of Law No. 8/1999 on Consumer Protection.[37,52] Under Article 75, which keeps existing personal-data rules in force only insofar as they do not conflict with UU PDP, sectoral rules (POJK 22/2023, Permenkes 24/2022) may validly set minimum archival floors (25-year medical records) and know-your-

customer (KYC) and clinical legal bases (Article 20(2)(c)), yet they cannot loosen the 3 × 24-hour clocks or the unbundling rules of UU PDP. Meanwhile the incident channels of OJK and Bank Indonesia (BI), the National Cyber and Crypto Agency (BSSN) with Komdigi, and UU PDP remain uncoordinated (PP No. 33/2026 Articles 114–115), which invites hedged breach clauses until coordination under Article 59(b) arrives. Article 74 made the duties binding on 17 October 2024. Even so, Articles 57(1) and 60 place administrative sanctioning solely with the Article 58 Agency, which has not been constituted, and that gap persisted after PP No. 33/2026 was promulgated on 16 July 2026. The teleological reading is blunt. A symbolic listing of rights (D3 = 100%), set beside 16.7% SLA compliance and 66.7% bundled consent, defeats informational self-determination over sensitive financial and clinical data. Last comes the historical reading. During the 2020–2022 legislative debates the executive insisted on an agency constituted by the President (Article 58(2)–(3)) instead of an independent statutory commission, and this may have contributed to multi-year administrative delay[5,14,53,54]. That delay could have signaled to controllers that refreshing inexpensive statutory citations (D1 = 43.3%) was cheaper than operational change.

4.2 The nullity paradox and the in terrorem effect

Automatic nullity under Articles 22(5) and 23 creates a nullity paradox of real force, much as it does in consumer standard-form contracting[37]. Batal demi hukum operates *ipso jure* and needs no court order. For that reason it sets off no administrative inspection by itself. A legally void text can still do behavioral work *in terrorem*, though. Suppose a borrower or telemedicine patient protests unsolicited cross-marketing or leakage of data to third parties. Customer-care teams may point to the bundled consent (66.7% of notices), the 10-day notice barrier, or the liability disclaimer (60.0%) set out in the privacy notice, which would discourage complaints before any tribunal can declare the clause void; evidence from residential leasing shows that consumers treat invalid terms as binding and forgo valid claims[55].

4.3 Comparative perspective: technique, sanction, and enforcement architecture

Table 9 and Figure 4 compare functional equivalents across five jurisdictions, and the comparison suggests that working supervisory machinery may matter more for compliance than the strictness of substantive rules. On paper, Indonesia's Law No. 27/2022 is stricter than Singapore's PDPA, which allows bounded deemed consent.[56] It is also stricter than GDPR Article 34 on direct 72-hour breach notification to subjects.[9,46] Singapore (PDPC) and Malaysia nonetheless gain operational traction. Malaysia's PDP Commissioner has enforced the mandatory DPO and 72-hour breach rules of Act A1727/2024 since June 2025.[57] In Singapore and Malaysia a standing regulator existed before commencement or arrived with it, and enforcement orders were published[46–48]; public disclosure of DPO contact details is mandated in Singapore (s. 11(3),(5)) and in Brazil (LGPD Art. 41 §1).[58] The PDPC keeps a public register of decisions and has imposed financial penalties,[59,60] and the Malaysian Commissioner reported raids on organizations processing personal data for commercial transactions in 2025.[61] These sources document enforcement activity, not compliance rates, which this study did not measure. Brazil's ANPD is the closest institutional analogue for Indonesia. After an initial executive delay (2018–2020), it adopted a mathematical Sanction Dosimetry Regulation (Resolution CD/ANPD No. 4/2023),[62] which operationalizes the 2% revenue cap (identical to UU PDP Art. 57(3)), together with a 3-working-day breach rule (Resolution No. 15/2024)[49,63]. By October 2026 the ANPD had concluded eight sanctioning proceedings and had 28 more under analysis.[64] Indonesia could adopt both elements through Presidential and Agency regulations, although imported rules work only as well as the local institutions that apply them.[65,66]

Table 9. Functional comparison of personal data protection enforcement architectures across five jurisdictions (November 2026).

Functional dimension	Indonesia (UU 27/2022 & PP 33/2026)	European Union (GDPR 2016/679)	Singapore (PDPA 2012, rev. 2020)	Malaysia (PDPA 2010, am. Act A1727/2024)	Brazil (LGPD 13.709/2018 & ANPD)
Consent unbundling & nullity	Explicit, distinguishable consent; bundled clauses void *ipso jure* (Arts. 22(1),(5), 23)	Anti-tying rule (Art. 7(4)); browse-wrap/pre-ticked invalid (Planet49)	Affirmative consent + bounded statutory deemed consent (ss. 15–15A)	No express ban on bundled consent; general consent and notice rules (ss. 6, 7, 38); explicit consent for sensitive data (s. 40)	Specific highlighted consent; generic authorizations void (Art. 8 §4)
Breach notification clock	≤ 3 × 24 h (72 h) written notice to both subjects & Agency (Art. 46(1); PP 33/2026)	≤ 72 h to DPA (Art. 33); "without undue delay" to high-risk subjects (Art. 34)	≤ 3 calendar days (72 h) to PDPC; prompt notice to affected individuals (s. 26D)	≤ 72 h to Commissioner + prompt subject notice (s. 12B, live Jun 2025)	3 working days to both ANPD & subjects (ANPD Res. 15/2024; Art. 48)
Mandatory DPO & public contact	Conditional on large-scale specific/monitoring data (Art. 53(1)); contact required (Art. 54)	Conditional on public body or large-scale special/monitoring data (Art. 37)	Universal for all organizations; business contact must be public (s. 11(3),(5))	Mandatory DPO + formal Commissioner registration (s. 12A, live Jun 2025)	Universal Encarregado; identity & contact public on website (Art. 41 §1)
Supervisory status & fines (Nov 2026)	Art. 58 Agency unconstituted; PP 33/2026 in vacatio to Jan 2027; zero Art. 57 fines	National DPAs + EDPB active since May 2018; fines up to 4% global turnover	PDPC active since 2013; monthly published decisions; fines up to 10% local turnover	Pre-existing Commissioner enabled immediate 2025 inspections & fines	ANPD active; Dosimetria (Res. 4/2023) enforces fines up to 2% revenue

Note. Comparison follows Zweigert and Kötz's functional-equivalence method across dimensions fixed before coding. Rows 1 to 3 correspond to the first three columns of Figure 4; row 4 corresponds to its last three columns (dedicated authority in force, *ex officio* audits, administrative fines). DPA = data protection authority; ANPD = *Autoridade Nacional de Proteção de Dados*; PDPC = Personal Data Protection Commission. The Malaysian cell for a statutory ban on bundled consent was changed from "Active" to "Absent": Act 709 contains no express prohibition of bundled consent, only general consent and notice rules (ss. 6, 7, 38) and explicit consent for sensitive data (s. 40).[67] No administrative fine under Article 57 UU PDP has been reported, because the supervisory agency does not yet exist.[18,19]

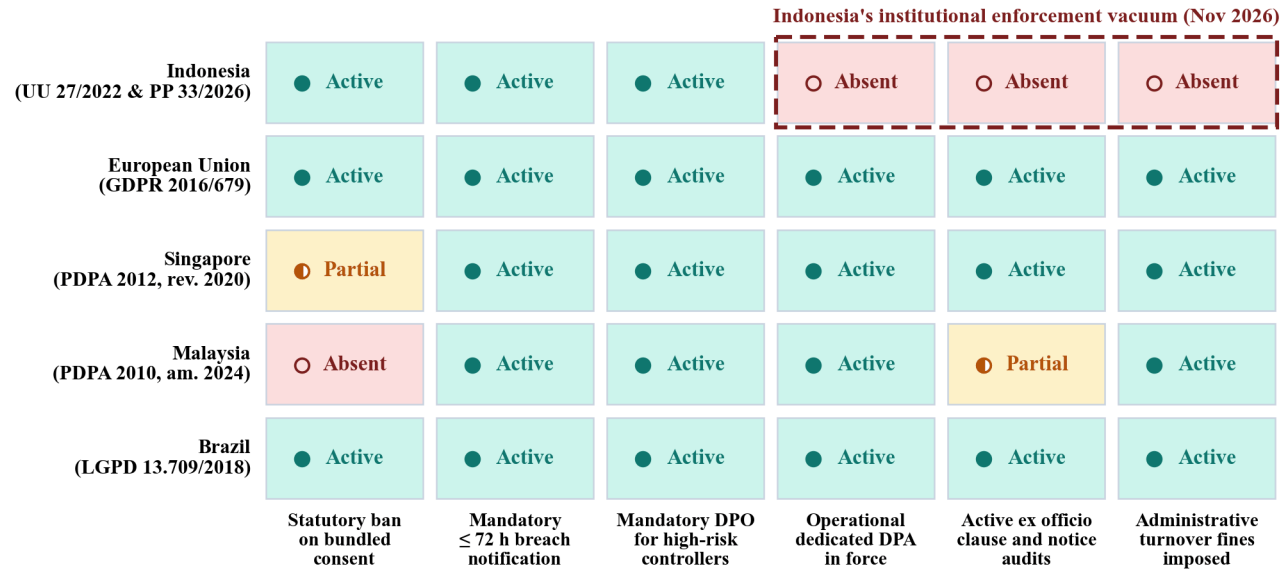

Figure 4. Comparative enforcement architecture across five personal data protection regimes as of November 2026; the dashed outline marks Indonesia's institutional enforcement vacuum. Symbols: filled circle = active, half-filled circle = partial, open circle = absent.

4.4 Limitations

Six limitations qualify these findings. The first concerns the sample. It is purposive (N = 30) and leaves out the JavaScript-rendered domains screened out *ex ante* (such as alodokter.com and bankjago.com), so that static HTML auditability could be preserved; the exclusion favors platforms with simpler sites. Prevalence estimates and binomial intervals thus describe the analyzed set, not national random-sample parameters, and larger future audits (N ≥ 100) should use headless browser rendering. Second, with n = 15 per sector the design can exclude large supervisory gaps (≥ 0.20 index points; MDE = 0.224), yet smaller divergences at the sub-indicator level need bigger samples. Third, public notices show normative text and not internal software-development-kit (SDK) traffic, so the 0.250 operational mean describes what notices state and not what platforms do; practice could be better or worse. Fourth, one coder carried out all coding. Deterministic rules and full release of the open data soften this, but scaled replications should use dual independent coders. Fifth, all notices were retrieved on a single date (16 November 2026), before PP No. 33/2026 takes operational effect, so the audit measures the position under Law No. 27/2022 alone. Sixth, A4 to A6 record whether a notice states duties that the statute triggers by event or threshold (a breach, large-scale processing of specific data, a cross-border transfer), so their absence from a notice is not in itself a violation.

4.5 De lege ferenda: five sequenced reform proposals

Table 10 sequences five reforms to close the +0.600 decoupling gap as PP No. 33/2026 enters into force on 16 January 2027 (Article 225). (1) The Article 58(5) Presidential Regulation on Lembaga PDP should be promulgated immediately, alongside an ANPD-style fine-dosimetry schedule (Article 57(3)). (2) A Mandatory Public DPO and Machine-Readable Notice Registry, audited by automated monthly crawlers, would eliminate blank emails (Eka Hospital), [ALAMAT] placeholders (Ciputra Hospital), and missing 3 × 24-hour clocks. (3) A Four-Authority Joint Supervisory Protocol (SKB Lembaga PDP–OJK–BI–Kemenkes) under Article 59(b) would embed A1–A6 (including maximum retention ceilings) into OJK Market-Conduct and Kemenkes SATUSEHAT renewals, with a Single-Window 3 × 24-Hour Breach Portal attached. (4) A Binding Administrative Blacklist would outlaw browsewrap consent, inseparable-T&C marketing bundling, inverted user notice clocks, and Force Majeure breach exonerations. (5) A Supreme Court Circular (SEMA) and a LAPS SJK Guideline would mandate *ex officio* nullity review of bundled privacy clauses under Articles 22(5) and 23.

Table 10. De lege ferenda: five sequenced institutional and regulatory reforms.

#	Reform proposal	Empirical defect targeted	Legal instrument required	Responsible body	Horizon
1	Constitute Lembaga PDP & issue 2% fine-dosimetry schedule	Zero Art. 57 enforcement; 0.250 operational mean	Perpres under Art. 58(5) & Agency Reg. under Art. 60 UU PDP	President of Indonesia; Setneg; Komdigi	Immediate (0–3 mos)
2	Establish public DPO & machine-readable privacy-notice registry	86.7% unreachable DPO (A5); blank/[ALAMAT] templates	Lembaga PDP Reg. implementing PP 33/2026 & Arts. 53–54	Lembaga PDP & Komdigi PSE Registry	Short (3–6 mos)
3	Enact Four-Authority Audit Protocol & Single-Window Breach Portal	Sectoral parity (p = 0.670); 86.7% missing 72 h breach clock	Joint Regulation (SKB) under Art. 59(b) UU PDP & PP 33/2026	Lembaga PDP, OJK, Bank Indonesia, Kemenkes	Short (3–9 mos)
4	Publish binding blacklist of prohibited bundling & exoneration clauses	66.7% void bundling (P1/P2); 60.0% exoneration (P4)	Lembaga PDP Circular & OJK/Kemenkes Conduct Directives	Lembaga PDP, OJK Market Conduct, Kemenkes	Medium (6–12 mos)

#	Reform proposal	Empirical defect targeted	Legal instrument required	Responsible body	Horizon
5	Mandate *ex officio* nullity review & controller consent burden-shifting	In terrorem deterrence of void *batal demi hukum* terms	*Surat Edaran Mahkamah Agung* (SEMA) & LAPS SJK Guideline	Supreme Court (Mahkamah Agung), BPSK, LAPS SJK	Structural (12–18 mos)

Note. Sequenced around the 16 January 2027 operational commencement of Government Regulation (PP) No. 33 of 2026 (Article 225). SEMA = *Surat Edaran Mahkamah Agung*; SKB = *Surat Keputusan Bersama*; LAPS SJK = *Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan*.

5. Conclusion

Law No. 27 of 2022 became fully binding under Article 74 twenty-five months ago. Even so, Indonesian Fintech and Health-Tech platforms that process specific financial and clinical data remain bound by statute yet unpoliced in practice. Thirty live notices (143,316 words) show near-universal declarative transparency (0.850) alongside severe operational non-compliance (0.250, $p < 0.0001$). Statutory citation was not significantly associated with operational compliance ($p = 0.197$). Consent-bundling clauses within the scope of Articles 22(5) and 23 appear in 66.7% of notices. Breach commitments of 3 × 24 hours and reachable DPOs are each omitted in 86.7% of notices, and the sector difference is small ($p = 0.670$; the interval excludes differences of 0.20 or more). PP No. 33 of 2026 supplies substantive rules, but rulemaking cannot by itself cure an institutional enforcement vacuum. Five steps (Table 10) would help to turn constitutional informational protection from symbolic prose into operational law: issuing the Article 58(5) Presidential Regulation to activate Lembaga PDP, deploying registry-based automated clause auditing, harmonizing sectoral supervision, publishing a blacklist of prohibited clauses, and enforcing *ex officio* nullity review.

Declarations

Ethics Approval and Consent

Not applicable. The study analyzed publicly available corporate legal documents and legislation and involved no human subjects, so ethics committee approval was not required.

Use of Artificial Intelligence

The authors declare that no generative artificial intelligence tools were used in the design, analysis, or writing of this manuscript.

Author Contributions

D.R.: Conceptualization, Methodology, Software, Investigation, Data curation, Formal analysis, Visualization, Writing – original draft. G.P.: Validation, Supervision, Writing – review & editing. Both authors reviewed and approved the final version of the manuscript.

Funding

None. This research received no external funding.

Competing Interests

None. The authors declare no competing interests. Platform names are reported solely to identify publicly posted legal documents analyzed for academic research.

Data Availability Statement

The de-identified dataset and the analysis scripts supporting the findings are available from the corresponding author on reasonable request.

Acknowledgments

None.

References

1. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945* [1945 Constitution of the Republic of Indonesia], Articles 28D(1) and 28G(1).
2. Syahwami S, Hamirul H. The erosion of privacy in the digital age: A constitutional challenge in Indonesia. Enigma Law. 2024;2(2):75–84. doi:10.61996/law.v2i2.56
3. Widodo JE, Suganda A, Darodjat TA. Data privacy and constitutional rights in Indonesia. PENA LAW Int J Law. 2024;2(2):1–12. doi:10.56107/penalaw.v2i2.187
4. Makarim E. Hybrid paradigm from European and America concerning privacy and personal data protection in Indonesia. Indones Law Rev. 2013;3(2):109–132. doi:10.15742/ilrev.v3n2.31
5. Budiman R. The development of personal data protection law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. J Smart Hukum. 2023;2(1):24–36. doi:10.55299/jsh.v2i1.1352
6. Priscyllia F. Perlindungan privasi data pribadi perspektif perbandingan hukum. Jatiswara. 2019;34(3):239–249. doi:10.29303/jtsw.v34i3.218
7. Yuniarti S. Perlindungan hukum data pribadi di Indonesia. BECOSS J. 2019;1(1):147–154. doi:10.21512/becossjournal.v1i1.6030
8. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* [Law No. 27 of 2022 on Personal Data Protection]. *Lembaran Negara Republik Indonesia* Tahun 2022 Nomor 196, *Tambahan Lembaran Negara* Nomor 6820.
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Off J Eur Union. 2016;L119:1–88.
10. Bangsu MNA, Brahmanto DE, Shifa A. Legal protection of personal data in Indonesia following the enactment of Law No. 27 of 2022 on Personal Data Protection. Adv Community Serv Res. 2026;4(2):210–224. doi:10.60079/acsr.v4i2.968
11. Simbolon VA, Juwono V. Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. Publik J Ilmu Adm. 2022;11(2):178–190. doi:10.31314/pjia.11.2.178-190.2022
12. Fitri DPRK, Widodo H, Hermono B. Cross-border personal data transfer requirements under Indonesia's Personal Data Protection Law: Normative clarity and legal protection. J Law Polit Humanit. 2026;6(5):3952–3965. doi:10.38035/jlph.v6i5.3528
13. *Peraturan Pemerintah Nomor 33 Tahun 2026 tentang Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* [Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection]. *Lembaran Negara Republik Indonesia* Tahun 2026 Nomor 88. Promulgated 16 July 2026; in force 16 January 2027.
14. Widjaja G, Cesarianti FM. *Urgensi pembentukan lembaga pengawas pelindungan data pribadi* di Indonesia berdasarkan Pasal 58 juncto Pasal 59 dan Pasal 60 *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. SINERGI J Ris Ilm. 2024;1(4):234–242. doi:10.62335/8qf44b59
15. Aqilah R, Weryanti D, Susanti P. *Tanggung jawab negara* mengenai pelindungan data pribadi berdasarkan *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. J Ilm Kutei. 2024;23(2):158–172. doi:10.33369/jik.v23i2.34476
16. Komdigi: Perpres lembaga pengawas PDP masuk tahap final [Internet]. Jakarta: Katadata; 2026 Nov 5. Available from: https://katadata.co.id/digital/teknologi/6aec368e80c97/komdigi-perpres-lembaga-pengawas-pdp-masuk-tahap-final
17. Kasus penyadapan dan urgensi pembentukan badan pelindungan data pribadi [Internet]. Jakarta: Kompas.com; 2026 Nov 5. Available from: https://nasional.kompas.com/read/2026/11/05/17254301/kasus-penyadapan-dan-urgensi-pembentukan-badan-pelindungan-data-pribadi
18. Rakhmayanti I. Lembaga perlindungan data belum ada di RI, padahal aturannya sudah ada [Internet]. Jakarta: CNBC Indonesia; 2026 Sep 16. Available from: https://www.cnbcindonesia.com/tech/20260916115609-37-768328/lembaga-perlindungan-data-belum-ada-di-ri-padahal-aturannya-sudah-ada
19. Adaptist Consulting. Indonesia's Personal Data Protection Law is fully enforceable. Its regulator still doesn't exist [Internet].

Adaptist Consulting; 2026 Aug 21. Available from: https://adaptistconsulting.com/reports/indonesias-pdp-law-is-fully-enforceable-without-regulator/

20. Theresa G, Marlyna H. Pelindungan data pribadi pada layanan pendanaan berbasis teknologi informasi pasca Undang-Undang Nomor 27 Tahun 2022 dan Undang-Undang Nomor 4 Tahun 2023. J Huk Pembang. 2024;54(2):345–366. doi:10.21143/jhp.vol54.no2.1631
21. Elsy ENA, Ravena D, Noor A. Patient data protection compliance model in electronic medical record systems following the implementation of the Personal Data Protection Law in Indonesia. Pena Justisia. 2026;25(1):616–627. doi:10.31941/pj.v25i1.7364
22. Bromley P, Powell WW. From smoke and mirrors to walking the talk: Decoupling in the contemporary world. Acad Manag Ann. 2012;6(1):483–530. doi:10.5465/19416520.2012.684462
23. Kern A, Laguecir A, Leca B. Behind smoke and mirrors: a political approach to decoupling. Organ Stud. 2018;39(4):543–564. doi:10.1177/0170840617693268
24. Waldman AE. Industry unbound: the inside story of privacy, data, and corporate power. Cambridge: Cambridge University Press; 2021. doi:10.1017/9781108591386
25. Cohen JE. Turning privacy inside out. Theor Inq Law. 2019;20(1):1–31. doi:10.1515/til-2019-0002
26. Solove DJ. Murky consent: an approach to the fictions of consent in privacy law. SSRN [preprint]. 2023:1–55. doi:10.2139/ssrn.4333743
27. Barocas S, Nissenbaum H. Big data's end run around anonymity and consent. In: Lane J, Stodden V, Bender S, Nissenbaum H, editors. Privacy, big data, and the public good. Cambridge: Cambridge University Press; 2014. p. 44–75. doi:10.1017/cbo9781107590205.004
28. Susser D. Notice after notice-and-consent: Why privacy disclosures are valuable even if consent frameworks aren't. J Inf Policy. 2019;9:148–173. doi:10.5325/jinfopoli.9.2019.0148
29. Cate FH, Mayer-Schönberger V. Notice and consent in a world of Big Data. Int Data Priv Law. 2013;3(2):67–73. doi:10.1093/idpl/ipt005
30. Sprigman CJ, Tontrup S. Privacy decision-making and the effects of privacy choice architecture: Experiments toward the design of behaviorally-aware privacy regulation. J Empir Leg Stud. 2024;21(3):577–631. doi:10.1111/jels.12391
31. Obar JA, Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Inf Commun Soc. 2020;23(1):128–147. doi:10.1080/1369118x.2018.1486870
32. Utz C, Degeling M, Fahl S, Schaub F, Holz T. (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). New York: ACM; 2019. p. 973–990. doi:10.1145/3319535.3354212
33. Degeling M, Utz C, Lentzsch C, Hosseini H, Schaub F, Holz T. We value your privacy ... now take some cookies: measuring the GDPR's impact on web privacy. In: Proceedings 2019 Network and Distributed System Security Symposium (NDSS). Reston: Internet Society; 2019. doi:10.14722/ndss.2019.23378
34. Matte C, Bielova N, Santos C. Do cookie banners respect my choice? Measuring legal compliance of banners from IAB Europe's Transparency and Consent Framework. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE; 2020. p. 791–809. doi:10.1109/sp40000.2020.00076
35. Nouwens M, Liccardi I, Veale M, Karger D, Kagal L. Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). New York: ACM; 2020. p. 1–13. doi:10.1145/3313831.3376321
36. Nouwens M, Kristensen JB, Maalt K, et al. A cross-country analysis of GDPR cookie banners and flexible methods for scraping them. In: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25). New York: ACM; 2025. p. 1–28. doi:10.1145/3706598.3713648
37. Rahayu D, Badruddin A, Wang E. Void by law, alive in practice: measuring prohibited standard clauses in twenty Indonesian digital-platform contracts under Article 18. Enigma Law. 2026;3(2):74–94. doi:10.61996/law.v3i2.126
38. Elsyra N, Syahwami, Sunaryo J, et al. Evaluating the effectiveness of legal frameworks in promoting integrity and preventing maladministration in public agencies in Jambi Province. Enigma Law. 2025;3(1):28–37. doi:10.61996/law.v3i1.87
39. Zuwanda ZS, Judijanto L, Khuan H, et al. Normative study of Law No. 27 of 2022 on the Protection of Personal Data and its impact on the fintech industry in Indonesia. West Sci Law Hum Rights. 2024;2(4):421–428. doi:10.58812/wslhr.v2i04.1367
40. Salsabila UA, Kharisma DB. Effectiveness of legal protection against misuse of personal data in peer-to-peer lending fintech services based on Law Number 27 of 2022 on Personal Data Protection. Int J Educ Res Soc Sci. 2026;7(1):47–56. doi:10.51601/ijersc.v7i1.1029
41. Fiorentina P, Sulistianingsih D, Niravita A, et al. Legal protection of consumer personal data in Indonesia fintech peer-to-peer lending pioneers. Pandecta Res Law J. 2022;17(2):307–312. doi:10.15294/pandecta.v17i2.40235
42. Mahottama AA, Winata IGS. Legal protection of patient personal data in telemedicine practice: Aligning the Health Law and the Personal Data Protection Law. J Indones Sos Sains. 2026;7(5):2552–2558. doi:10.59141/jiss.v7i5.2332
43. Kemalasari NPY, Putra IPHS. Protection of medical record data as a form of legal protection of health data through the Personal Data Protection Act. J Digit Law Policy. 2023;2(3):111–118. doi:10.58982/jdlp.v2i3.338
44. Pakpahan JM. *Kesadaran urgensi peran pengendali dan prosesor data pribadi* dalam rangka pelindungan data pribadi individu berdasarkan *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. J Huk to-ra. 2024;10(1):119–137. doi:10.55809/tora.v10i1.331
45. Greenleaf G. Asian data privacy laws: trade and human rights perspectives. Oxford: Oxford University Press; 2014. doi:10.1093/acprof:oso/9780199679669.001.0001
46. Wong BYQ. Data privacy law in Singapore: The Personal Data Protection Act 2012. Int Data Priv Law. 2017;7(4):287–302. doi:10.1093/idpl/ipx016
47. Shabudin NMB, Yi CE. Malaysia. In: Privacy and personal data protection law in Asia. Oxford: Hart Publishing; 2024. p. 169–200. doi:10.5040/9781509965502.ch-007
48. Hoang Le M. From fragmentation to interoperability: How the GDPR shapes ASEAN data privacy and cross-border data flows. J Data Prot Priv. 2026;8(3):236–252. doi:10.69554/jyui7132
49. Divino SBS. *Comunicação de incidentes de segurança*: Prazo, regulatory enforcement e a competência da *Autoridade Nacional de Proteção de Dados*. *Rev Direito Adm*. 2023;282(3):143–175. doi:10.12660/rda.v282.2023.90158
50. *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis* [Minister of Health Regulation No. 24 of 2022 on Medical Records], Article 39.
51. *Kitab Undang-Undang Hukum Perdata* (*Burgerlijk Wetboek*) [Indonesian Civil Code], Articles 1320 and 1337.
52. *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen* [Law No. 8 of 1999 on Consumer Protection], Article 18.
53. Widiatedja IGNP, Mishra N. Establishing an independent data protection authority in Indonesia: a future-forward perspective. Int Rev Law Comput Technol. 2022;37(3):252–273. doi:10.1080/13600869.2022.2155793
54. Sihombing AB. Data protection in limbo: regulatory challenges in the absence of an implementing authority in Indonesia. SENTRI J Ris Ilm. 2025;4(11):3656–3667. doi:10.55681/sentri.v4i11.4965
55. Furth-Matzkin M. On the unexpected use of unenforceable contract terms: evidence from the residential rental market. J Leg Anal. 2017;9(1):1–49. doi:10.1093/jla/lax002
56. Parliament of Singapore. Personal Data Protection Act 2012 (Act 26 of 2012), as amended by the Personal Data Protection (Amendment) Act 2020.
57. Parliament of Malaysia. Personal Data Protection Act 2010 (Act 709), as amended by the Personal Data Protection (Amendment) Act 2024 (Act A1727).
58. República Federativa do Brasil. *Lei nº 13.709, de 14 de agosto de 2018* (*Lei Geral de Proteção de Dados Pessoais*, LGPD).
59. Personal Data Protection Commission (Singapore). Enforcement decisions [Internet]. Singapore: PDPC; 2026 [updated 2026 May 7]. Available from: https://www.pdpc.gov.sg/all-commissions-decisions
60. Baker McKenzie. Singapore: PDPC fines several organizations [Internet]. Baker McKenzie; 2026 Jan 30. Available from: https://www.bakermckenzie.com/en/insight/publications/2026/01/singapore-pdpc-fines-several-organizations
61. Kementerian Digital perkenal sistem perisikan pantau aktiviti jual data peribadi [Internet]. Sinar Harian (Bernama); 2025 Feb 18. Available from: https://www.sinarharian.com.my/article/713439/berita/nasional/kementerian-digital-perkenal-sistem-perisikan-pantau-aktiviti-jual-data-peribadi
62. *Autoridade Nacional de Proteção de Dados*. *Resolução CD/ANPD* nº 4, de 24 de fevereiro de 2023: *Regulamento de Dosimetria e Aplicação de Sanções Administrativas*.
63. *Autoridade Nacional de Proteção de Dados*. *Resolução CD/ANPD* nº 15, de 24 de abril de 2024: *Regulamento de Comunicação de Incidente de Segurança*.

64. *Autoridade Nacional de Proteção de Dados*. Balanço ANPD 6 anos 2020–2026 [Internet]. Brasília: ANPD; 2026 Oct. Available from: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/balanco-anpd-6-anos.pdf
65. Berkowitz D, Pistor K, Richard JF. Economic development, legality, and the transplant effect. Eur Econ Rev. 2003;47(1):165–195. doi:10.1016/s0014-2921(01)00196-9
66. Teubner G. Legal irritants: good faith in British law or how unifying law ends up in new divergences. Mod Law Rev. 1998;61(1):11–32. doi:10.1111/1468-2230.00125
67. Paulger D. ABLI-FPF Convergence Series: Malaysia – status of consent for processing personal data [Internet]. Future of Privacy Forum, Asian Business Law Institute; 2022 Jul. Available from: https://fpf.org/wp-content/uploads/2022/07/ABLI-FPF-Consent-Project-Malaysia-Jurisdiction-Report.pdf