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

e-ISSN 3026-6068
Vol. 4, No. 1 (2026) · pp. 40–49

ORIGINAL RESEARCH ARTICLE

The Illusion of Free Consent: A Cross-Jurisdictional Content Analysis of Digital Consent Architecture and Indonesia's Personal Data Protection Law

Hesti Putri[1*], Henry Peter Paul[2], Fitriyanti Fitriyanti[3]

[1] *Department of Informatics Science, CMHC Research Center, Palembang, Indonesia*
[2] *Department of Behavior Economy, Miami History Museum, Miami, United States*
[3] *Department of Regional Economics, Enigma Institute, Palembang, Indonesia*

ARTICLE INFO

Received: March 5, 2026
Revised: April 25, 2026
Accepted: May 19, 2026
Available online: June 16, 2026
Published: June 30, 2026
Keywords Free consent; Standard-form contracts; Dark patterns; Data protection; GDPR; UU PDP; Enforcement
Correspondence Hesti Putri · hesti.putri@gmail.com
ORCID 0009-0002-9568-3731
DOI
https://doi.org/10.61996/law.v4i1.152

ABSTRACT

Background. Data-protection regimes make consent their main lawful basis, assuming that a user who clicks 'I agree' on a standard-form interface has chosen freely.

Objective. This article tests that assumption empirically. It asks how far the consent interfaces of widely used digital platforms meet the legal conditions of valid consent, how they differ across regulatory regimes, and what this implies for Indonesia.

Methods. In a structured content analysis, the primary consent interface of forty digital platforms (social, e-commerce, streaming, news, fintech and software-as-a-service; European, Indonesian and South-East-Asian regimes) was coded against ten binary indicators of consent validity derived from Articles 4(11) and 7 of the General Data Protection Regulation (GDPR), European Data Protection Board guidance and the Planet49 ruling, and summed into a Free Consent Index (0–10).

Results. The distribution was strongly bimodal (mean 6.85, SD 3.68, median 8.5). Only eighteen of forty platforms (45%) offered genuine free consent; the rest showed nudged (11), coerced (4) or illusory (7) consent. GDPR-tier flows averaged 8.12 against 1.75 for Indonesian and regional local flows (Mann–Whitney $p < 0.0001$), whereas advertising funding was not associated with the index ($p = 0.94$). Even under the GDPR, genuine consent was not universal, and compliant interfaces often belonged to platforms already under enforcement.

Conclusion. The study offers a reproducible instrument and a jurisdiction-linked typology. Jurisdictional flow was most strongly associated with the index, and free consent may depend on credible enforcement more than on the drafter's good faith, which matters for Indonesia's newly enforced data-protection law.

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

Personal-data protection law rests on an act of clicking. In the world's data-protection statutes, which include the European Union's General Data Protection Regulation (GDPR),[1] California's privacy legislation, Brazil's LGPD, China's PIPL, and, most recently, Indonesia's Law No. 27 of 2022 on Personal Data Protection (*Undang-Undang Pelindungan Data Pribadi*, 'UU PDP'),[2] consent is the primary legal basis. It turns an intrusion into personal life into a lawful transaction. A user who ticks a box or presses 'I agree' is deemed to have exercised autonomy. The user is presumed to have read, understood, weighed and freely accepted the terms on which data will be collected, combined, inferred from, and monetized. That presumption is the doctrinal cornerstone on which much of the digital economy legally rests, and this article puts the cornerstone to an empirical test [3].

The article also argues that this cornerstone is frequently a fiction. Digital consent is obtained through standard-form contracts of a peculiarly modern kind. They are non-negotiable and drafted entirely by the data controller. They appear at the threshold of a service the user has already resolved to use, and they are engineered by designers whose commercial interest lies in maximizing the flow of data [4,5]. The law demands consent that is 'freely given, specific, informed and unambiguous'. The lived reality is a cookie banner whose 'Accept all' button glows while its 'Reject' option sits buried three layers deep. That gap is no accident. Deliberate choice architecture

produces it, and the law now has a name for the techniques that exploit it: dark patterns [5,6].

How far that gap is bridged differs from one part of the globe to another. A single platform may present a scrupulously symmetric consent screen to a user in Frankfurt and no consent screen at all to a user in Jakarta. A national news site in one jurisdiction may run an elaborate consent-management platform, while its counterpart in another tracks every reader with no consent moment whatsoever [7–9]. The article exploits this variation as its empirical opening. Honest drafting alone would produce similar screens everywhere. They do not look alike, which suggests that the true determinants lie elsewhere: in the regulatory regime, the credible threat of enforcement, and the business model [10,11].

For Indonesia the question is neither abstract nor academic. Article 28G(1) of the 1945 Constitution[12] guarantees every person 'protection of self, family, honour, dignity, and property', and doctrine reads this provision as the constitutional seat of informational privacy [13]. On that foundation, UU PDP No. 27 of 2022 imports a GDPR-style consent standard, one that is explicit, specific, informed and unambiguous under Articles 20–22. Enforcement began in October 2024, when the two-year transition period in Article 74 expired. The statute now meets the standard-form consent practices that this study catalogues. The pressing legal question is simple: will a consent standard on paper, by itself, dislodge them [14]?

This article makes three contributions. The first is a reproducible measurement instrument, the Free Consent Index. It operationalizes each limb of the legal doctrine of valid consent as a discrete, falsifiable coding test, and it translates Articles 4(11) and 7 GDPR and the guidance of the European Data Protection Board (EDPB) into ten binary indicators.[15,16] Second, the article supplies a jurisdiction-linked typology. This typology separates genuine choice from its three counterfeits, namely nudged, coerced and illusory consent, and relates them empirically to the jurisdiction of the platform's consent flow [17]. Third, and with *de lege ferenda* intent, the article draws three concrete reform proposals from the cross-jurisdictional evidence. They are addressed to the Indonesian institutions now charged with giving the UU PDP practical effect.

The remainder of the article is organized as follows. Sections 1.1 to 1.3 set out the legal and theoretical framework: the anatomy of valid consent, the dark-patterns doctrine, and the Brussels-effect thesis. Section 2 states the empirical socio-legal methodology, the coding instrument, and the reliability procedure. Section 3 reports the results. In Section 4 the findings are discussed and read against the interpreted text of the GDPR and the UU PDP, the reform agenda is developed, and the study's limitations are recorded. Section 5 concludes.

1.1 The legal anatomy of valid consent

The GDPR does not treat consent as a mere formality. Article 4(11) defines it as a 'freely given, specific, informed and unambiguous indication' of the data subject's wishes, given by 'a clear affirmative action'. Article 7 adds two points: consent bundled into the acceptance of a service, or made a condition of a service that does not require it, is, under Article 7(4) and Recital 43, treated as presumptively not freely given, and withdrawal must be as easy as giving. In *Planet49* (C-673/17)[18] the Court of Justice held that a pre-ticked box cannot constitute valid consent, since silence or inactivity is not an affirmative act. The EDPB's Guidelines 05/2020 on consent,[19] together with its Guidelines 03/2022 on deceptive design patterns,[20] translate these abstractions into interface requirements. They call for a first-layer means to refuse, no pre-selected non-essential options, granularity of purpose, and no manipulative nudges.[15] Indonesia's UU PDP mirrors the substance. Article 20(2)(a) requires consent that is explicit and given for one or more specified purposes, and Articles 21–22 condition its validity, all on a constitutional foundation in Article 28G(1) of the 1945 Constitution [13].

These conditions can be read as a set of structural tests. A consent interface either passes or fails each one, and that is what makes the doctrine amenable to measurement. A valid-consent interface must offer a real and symmetric choice to refuse. It must not pre-select the user's agreement, and it must let the user distinguish among purposes. It must not hold the service hostage to consent, and it must separate consent from the general contract. Withdrawal has to be painless. Information must reach the user at the point of decision, and the interface must disclose who receives the data. Design must not deceive. Finally, a want of consent must not hide behind a misdescribed legal basis. The Free Consent Index operationalizes these ten tests, which are set out in full in Table 1.[15,21]

1.2 Dark patterns and the manufacture of assent

Behavioral-design scholarship and regulators now agree that consent interfaces are frequently engineered not to elicit a decision but to manufacture one. Confirmshaming, false hierarchy, obstruction, nagging and pre-selection are the documented techniques.[5,6,22] The EDPB's dark-patterns taxonomy points the same way, as do several enforcement actions: the CNIL's fines against Google and Facebook (2021) and against TikTok and Microsoft (2022) for refusal mechanisms harder to use than acceptance,[23–26] and its 2020 fines against Google and Amazon for cookies set without prior consent,[27,28] the Belgian regulator's ruling that the advertising industry's Transparency and Consent Framework could not yield valid consent,[29] (a ruling that the Brussels Market Court annulled on procedural grounds on 14 May 2025 while substituting its own decision, which confirmed the fine and the joint-controller finding for the TC String preferences)[30] and the EDPB's Opinion 08/2024 that the 'pay-or-consent' model of large online platforms generally cannot.[31] Together they establish that these are legal defects, not merely design infelicities [32]. Experimental and field work shows that the techniques measurably shift outcomes. Highlighting 'accept' and burying 'reject' raises consent rates regardless of preference.[16,33,34] Large-scale audits find that most banners nudge users toward acceptance.[7,16,35] The theoretical claim tested here is that such defects are structural rather than exceptional. Absent regulatory pressure, the standard-form digital consent interface tends toward the illusion of free consent, not its substance.

1.3 The Brussels effect and its limits

A competing possibility is that the problem corrects itself. The 'Brussels effect' thesis holds that global platforms find it cheaper to apply the strictest applicable standard everywhere.[36] On that view, the GDPR's demanding consent rules spread worldwide and raise consent quality even in jurisdictions with weaker laws. The cross-jurisdictional design here offers an indirect test of the thesis, because it compares different platforms rather than one platform across jurisdictions. Suppose the Brussels effect were strong: the consent architecture a platform presents in a weak-law jurisdiction should then resemble the one it presents in the EU. Suppose instead that platforms geo-tailor their interfaces, offering full compliance where the regulator has teeth and a bundled or absent consent moment where it does not. Diffusion is then partial at best. The protection a user enjoys would depend less on the platform than on the platform's estimate of where that user can complain [8,10].

2. Methods

2.1 Research type and justification

This is an empirical socio-legal study. It pairs doctrinal legal analysis with a structured, deductive quantitative content analysis of legal-technical artifacts. The doctrinal component interprets the primary law of consent (the GDPR, the UU PDP, and the relevant jurisprudence) to derive the normative

benchmark against which practice is measured, and the empirical component then observes and codes, interface by interface, how far real interfaces satisfy that benchmark. The design is justified because the research question is relational rather than purely doctrinal or purely empirical. It asks how far observable practice conforms to interpreted doctrine, and what explains the divergence. Theory-driven content analysis is widely used in the privacy-engineering literature.[11,16,21,37] It fits. It makes that relation measurable and reproducible.

2.2 Legal-interpretive approach

The doctrinal benchmark was built with the classical methods of statutory interpretation, applied in sequence. Grammatical interpretation came first. It fixed the ordinary meaning of the operative terms: Article 4(11) GDPR defines consent as a 'freely given, specific, informed and unambiguous indication' given by 'a clear affirmative action', and Article 20(2)(a) UU PDP mirrors this by requiring valid, explicit (*eksplisit*) consent given for one or more specified purposes. Systematic interpretation then read these definitions alongside their neighboring provisions, namely Article 7(3)–(4) GDPR and Articles 20–24 UU PDP, which allowed consent to be reconstructed as a set of cumulative structural conditions rather than a single formality. Teleological interpretation asked what those conditions are for. Recitals 32, 42 and 43 GDPR and the *naskah akademik* of the UU PDP show a purpose of protecting informational self-determination, and that purpose is frustrated wherever assent is manufactured rather than chosen [3]. Last came historical interpretation. It placed the standard within the Court of Justice's development of it, from the pre-ticked box invalidated in *Planet49* (C-673/17) to *Meta v Bundeskartellamt* (C-252/21),[38] in which dominance weighed on the assessment of whether consent was freely given.

2.3 Sample and legal sources

The sample comprises forty digital platforms. They were purposively selected to span sectors (social/messaging, e-commerce, streaming, travel, news, fintech, SaaS), operator domiciles (United States, EU/UK, China, South-East Asia and Indonesia), and governing regimes. Globally dominant services running a GDPR-tier consent flow sit beside Indonesian and regional platforms governed mainly by the UU PDP or Singapore's PDPA,[39] so the cross-jurisdictional contrast sits inside the sample itself. Selection was purposive, not probabilistic. Its aim is variation, not representativeness. The coding standard came from primary legal sources: the GDPR, the UU PDP, the 1945 Constitution, GR 71/2019,[40] the CJEU jurisprudence, the EDPB guidelines and opinions, and the enforcement decisions of the CNIL and the Belgian DPA. The peer-reviewed privacy-engineering and doctrinal literature informed the operationalization [5,41].

2.4 Coding instrument and analysis

Each platform's primary consent interface was coded for the ten binary indicators listed in Table 1, which were summed into the Free Consent Index (FCI, 0–10). Coding drew on several sources: the platform's live consent banner where observable, its published privacy and cookie policies, decisions of national data-protection authorities, complaints and audits by the privacy NGO noyb and the consumer organization BEUC, and EU enforcement records. Every non-obvious code is backed by a documented source recorded in the dataset. Where a platform operates a stronger EU flow and a weaker non-EU flow, the coded indicators reflect the flow that its dominant relevant user encounters, while the geographic divergence is kept as qualitative evidence. Uncertain or unverifiable features were coded 0. That conservative rule understates GDPR-tier scores and may equally understate the scores of local platforms, whose public documentation is thinner. Group differences were tested with the Mann–Whitney U and Kruskal–Wallis tests, using exact distribution functions suited to the small, bounded, non-normal index. The z values reported in Section 3.2 are tie-corrected normal approximations, and a permutation test on the plotted platform scores also gives $p < 0.0001$. Effect sizes are reported as rank-biserial correlations.

Table 1. The ten consent-validity indicators of the Free Consent Index.

Code	Indicator	Legal condition tested
F1	Symmetric reject	'Reject all' on the first layer, of equal prominence to 'Accept' (freely given; Art. 7)
F2	No pre-selection	Non-essential options default off; no pre-ticked consent (*Planet49*, C-673/17)
F3	Granular control	Consent per purpose/vendor, not all-or-nothing (specific; Art. 4(11))
F4	No consent wall	Service usable without consenting; no forced or 'pay-or-consent' wall (Art. 7(4))
F5	Unbundled	Tracking consent separate from acceptance of the general terms (Art. 7(4))
F6	Easy withdrawal	Persistent mechanism to withdraw, as easy as giving (Art. 7(3))
F7	Informed at point	Purposes disclosed in plain language at the moment of consent (informed)
F8	Recipients disclosed	Controller and third-party recipients named before consent (Arts 13–14)
F9	No deceptive design	No confirmshaming, nagging, obstruction or visual steering (EDPB 03/2022)
F10	Legal-basis honesty	Tracking on consent, not covert 'legitimate interest' (IAB TCF decision)

Note. Each indicator is coded present (1) or absent (0); the Free Consent Index is their sum (0–10). F = indicator; Art. = Article of the GDPR; EDPB = European Data Protection Board; IAB TCF = Interactive Advertising Bureau Transparency and Consent Framework.

Platforms were then mapped to a four-part typology of consent architecture, summarized later in Table 2. A regime counted as genuine choice when it met the core freely-given conditions (symmetric reject, no wall, unbundled) and also showed honest, non-deceptive design and a high index (F1, F4, F5, F9 and F10 all present and FCI ≥ 8; because these five indicators are also components of the FCI, the separation of the types by FCI in Figure 3B follows partly from the definition). Some regimes presented no functional consent interface at all. Their consent was either bundled into a 'by using this service you agree' model or replaced by covert tracking with no consent moment, and these were classed as illusory consent. Where an interface existed but consent was extracted as a precondition of the service, the regime was classed as coerced consent. The rest offered a genuine option to refuse. Yet they degraded it through dark patterns, asymmetry or a dishonest legal basis, and they were classed as nudged consent [42].

2.5 Reliability and research ethics

A blind second coder independently re-coded a subsample of ten platforms (one hundred indicator judgments). The

subsample was deliberately drawn from the most interpretively contested cases: pay-or-consent flows, app-onboarding flows and advertising-framework news banners. Raw agreement was 70%. Cohen's kappa was 0.38 (95% CI 0.20–0.57), 'fair' on the conventional Landis–Koch benchmark, and the limitations discuss this candidly.

2.6 Formal definition, scope and worked interpretation

Formally, the Free Consent Index is the unweighted sum of the ten binary indicators of Table 1:

$$FCI = \Sigma F_i, \quad i = 1, \ldots, 10, \quad \text{with each } F_i \in \{0, 1\}$$

giving a theoretical and observed range of 0–10. Equal weighting embeds an assumption that each cumulative condition of valid consent contributes equally to freeness. That is contestable in law. The results were therefore checked, by rebuilding the index, against two theoretically motivated alternative weightings: double-weighting the 'freely given' indicators F1 and F4, and a disclosure-versus-control split. The jurisdictional contrast and typology were stable under both. The indicators are pitched at the GDPR's context-independent consent conditions (Art. 4(11)/7) and not at the cookie-specific ePrivacy trigger, and for that reason coding a registration or onboarding flow against F1–F10 is doctrinally coherent across contexts [43].

Article 7(4) GDPR serves as a worked example of the interpretive derivation. Four readings apply. The grammatical reading fixes 'freely given' as excluding a choice that carries a penalty for refusal. The systematic reading places Article 7(4) beside Article 4(11)'s 'clear affirmative action' and Article 7(3)'s withdrawal rule, and treats bundling and conditionality as defeating freeness. The teleological reading, by reference to Recitals 42–43, identifies the protected interest as informational self-determination, which a consent wall frustrates, and the historical reading traces the standard from *Planet49* (C-673/17) to *Meta v Bundeskartellamt* (C-252/21), in which the Court held that a dominant position does not as such prevent valid consent but is an important factor in assessing whether it was freely given. Together these readings generate indicators F1 (symmetric reject), F4 (no consent wall) and F5 (unbundled). The coding frame is derived from the interpretive methods. It is not merely labeled with them.

Two indicators need a decision rule. It converts a legal judgment into a binary code. F10 (legal-basis honesty) received 0 where non-essential tracking rested on a 'legitimate interest' basis of a kind that the EDPB or a competent DPA has rejected in materially similar circumstances [44]. F9 (no deceptive design) received 0 where the interface showed at least one technique from the taxonomy in the EDPB's Guidelines 03/2022 (confirmshaming, false hierarchy, obstruction, nagging or pre-selection). Interfaces were observed during a defined collection window and from a stated vantage point, archived policy snapshots were retained, and, for independent verification, the coding manual, the full 40 × 10 matrix with per-code sources and timestamps, the reliability key and the seeded analysis script are deposited as supplementary materials [35].

3. Results

3.1 Genuine consent is the exception

The Free Consent Index averaged 6.85 of 10 (SD 3.68) across the forty platforms. The mean misleads, though, because the distribution is strongly bimodal. As Figure 1 shows, the median is 8.5, and platforms cluster either near the top of the scale or at its floor, with little in between. The individual indicators explain why. Figure 2 presents the prevalence of each of the ten indicators, split by jurisdictional flow. Disclosure and choice features were common overall: an absence of a hard consent wall (80%), disclosure of recipients (80%), and informedness at the point of consent (78%). The two features that most directly secure a free choice were scarcest. A symmetric first-layer option to reject appeared in only 52.5% of interfaces, and the absence of deceptive design in only 52.5%. Barely half of the forty platforms in this purposive sample, then, let the user refuse as easily as accept, or did so without manipulation. The prevalence matches the web-scale audits of the recent literature [7,11].

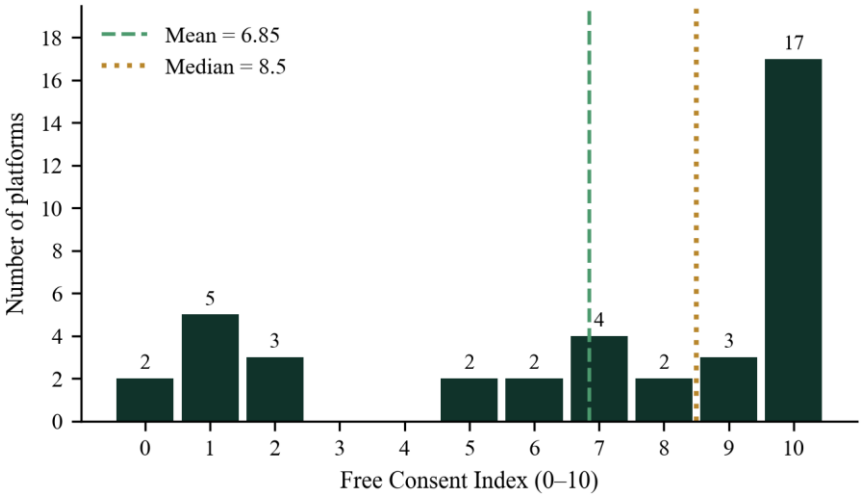

Figure 1. Bimodal distribution of the Free Consent Index across the forty platforms (mean 6.85; SD 3.68; median 8.5), showing clustering at the ceiling and the floor.

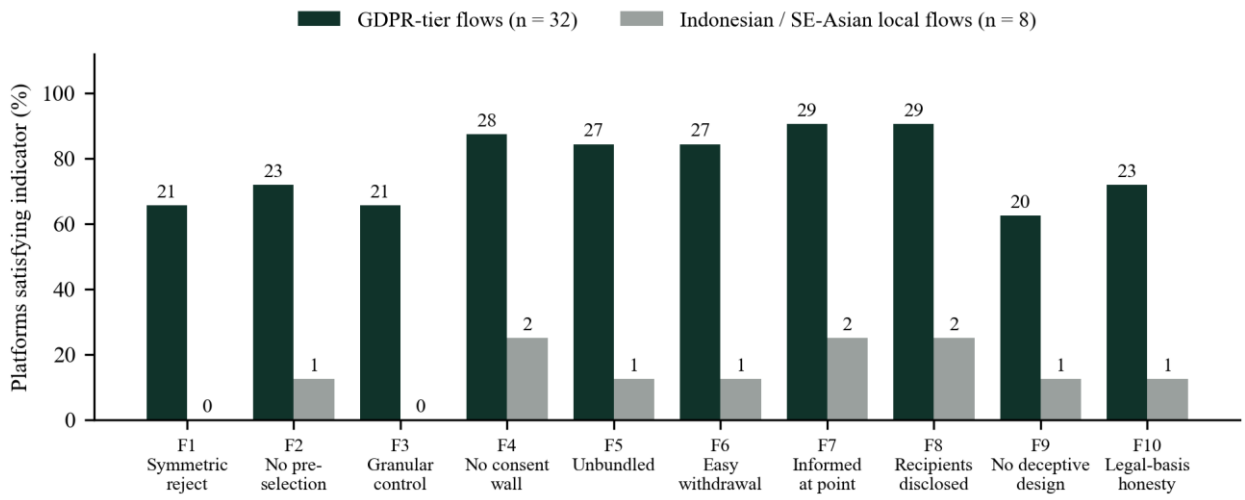

Figure 2. Prevalence of each consent-validity indicator (F1–F10) among GDPR-tier flows (n = 32) versus Indonesian and South-East-Asian local flows (n = 8); numbers above the bars are counts of platforms.

Table 2 details the typology, which sharpens the point. Genuine free consent, meaning a symmetric, unbundled, non-coercive and non-deceptive interface, characterized only 18 of the 40 platforms (45%; mean FCI 9.94). The majority, 55%, presented one of three counterfeits. Eleven platforms offered nudged consent (mean 7.00). A real reject option existed there, but asymmetry, dark patterns or a dishonest legitimate-interest default degraded it. Most advertising-funded news sites follow this pattern, as do platforms such as Netflix, Booking.com and Temu, whose written policies read as compliant while their interfaces steer.[37,44,45] Four presented coerced consent (mean 2.75): a consent interface existed, but agreement was the price of the service, as in Meta's 'pay-or-consent' model, WhatsApp's forced 2021 terms update, and Grab's onboarding. Seven presented illusory consent (mean 1.00). There was no functional consent interface at all; the user was deemed to consent merely by using the service, or was tracked with no consent moment whatsoever [8].

Table 2. Typology of consent architecture across the forty platforms.

Type	n	Mean FCI	Character of the consent
Genuine choice	18	9.94	Freely given; a real, symmetric option to refuse
Nudged consent	11	7.00	Choice exists but is steered or deceived by design
Coerced consent	4	2.75	Agreement is extracted as the price of the service
Illusory consent	7	1.00	No functional consent interface at all

Note. Coerced: Meta/Facebook, Instagram, WhatsApp, Grab. Illusory: Shopee, Tokopedia, Lazada, Kompas.com, Detik.com, Gojek/GoPay, DANA. Nudged includes Netflix, Booking.com and Temu (Section 3.1). FCI = Free Consent Index.

3.2 Jurisdiction, not business model, is the determinant

What separates the top of the distribution from the floor is jurisdiction, not sector or business model. As Figure 3 (panel A) shows, platforms operating a GDPR-tier consent flow scored 8.12 on average, while the eight Indonesian and South-East-Asian platforms coded on their local flow scored 1.75. That gap exceeds six points on a ten-point scale and is among the largest and most significant contrasts in the study (Mann–Whitney $U = 15$, $n = 32$ and 8, $z = -4.00$, $p < 0.0001$). Recomputed from the platform scores plotted in Figure 3, the tie-corrected z is −3.93 and a permutation test gives $p < 0.0001$, so the conclusion does not depend on the normal approximation; U computed from the plotted points is 16.5 rather than 15, a difference of one or two ranks that the 40 × 10 matrix should settle. Panel B of the same figure resolves the index by architecture type, and the four typological clusters separate, as expected because the types are partly defined from index components (Section 2.4). Without exception, the seven illusory-consent platforms are Indonesian or regional services; together with Grab, classed as coerced, they make up the eight local-flow platforms, so the illusory type and the local group largely describe the same platforms. Three are marketplaces (Shopee, Tokopedia, Lazada) that fold consent into their terms of use; two are national news sites (Kompas, Detik) that run advertising trackers behind no consent interface at all; two are domestic e-wallets (Gojek/GoPay, DANA) that treat registration as consent. For an Indonesian user, whether anything resembling free consent protects their data appears to depend largely on whether the service they open was built for Brussels or for Jakarta.[9,14,46]

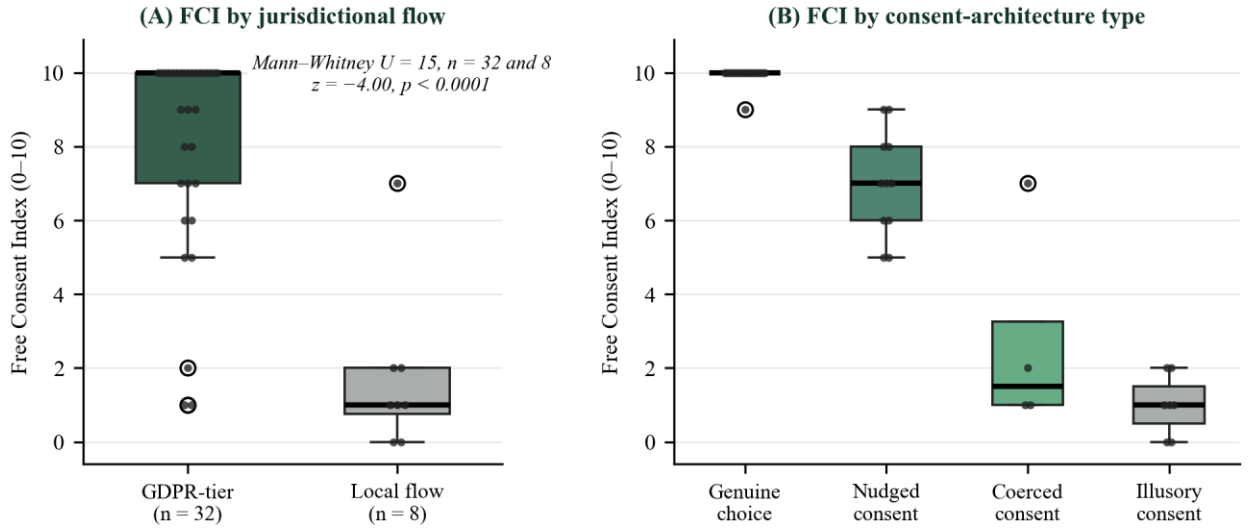

Figure 3. Free Consent Index by jurisdictional flow (panel A) and by consent-architecture type (panel B). Boxes show median and interquartile range; whiskers extend to 1.5 × IQR; open circles mark outliers; points are individual platforms.

Two comparisons are compatible with a regulatory rather than a commercial explanation. First, business model was not associated with consent quality. Advertising-funded platforms, the sector one might expect to extract consent most aggressively, scored no worse than the rest (6.94 versus 6.77, p = 0.94), and sector differences overall were not significant (Kruskal–Wallis p = 0.14). The productivity-software sector scored highest (mean 10.0). That reflects no special virtue among such firms: they depend least on behavioral advertising and have been swept up in the same EU enforcement. Second, the several China-origin platforms exposed to EU enforcement (TikTok, AliExpress, Temu) present better consent flows than the Indonesian platforms that are not. This is compatible with the reach of the regulator, rather than the domicile of the firm, mattering.[10,47]

3.3 The illusion persists even under the GDPR

It would be too comfortable to conclude that the GDPR has solved the problem and that only weak-law jurisdictions lag. The illusion is present even within the 32 GDPR-tier flows. Their mean of 8.12 falls well short of the ceiling. Only 53% achieved a perfect score, and only 56% qualified as genuine consent. As Figure 2 makes visible, a symmetric first-layer reject was present in only 66% of GDPR flows, and legal-basis honesty in only 72%, so roughly a third of the most heavily regulated consent interfaces in the world still either hide the reject button or lean on a 'legitimate interest' to preselect tracking [32,44]. The compliant flows are also disproportionately those forced into compliance. Google, Amazon, Microsoft and TikTok all score at or near the top, and each was fined by a national regulator. The CNIL fined Google and Amazon on 7 December 2020,[27,28] Google and Facebook on 31 December 2021,[23,24] and Microsoft and TikTok on 19 and 29 December 2022.[25,26] The Microsoft and TikTok decisions record that a one-click 'refuse all' button was introduced on 29 March 2022 and 28 February 2022 respectively. The picture is of a norm imposed, not internalized, and imperfectly, one enforcement action at a time. Meanwhile the frontier of circumvention moves on to the 'pay-or-consent' wall that the EDPB has had to address in turn.[45,48]

3.4 Reliability

Inter-coder reliability on the contested subsample was fair. Raw agreement reached 70% and Cohen's kappa = 0.38 (95% CI 0.20–0.57), 'fair' on the conventional Landis–Koch benchmark. That is lower than is comfortable, so it is reported plainly rather than buried. Two features explain and bound it. First, the subsample was deliberately composed of the hardest cases: pay-or-consent screens, app-onboarding flows, and advertising-framework news banners, on which reasonable coders genuinely differ. Agreement on the many clear cases (uniform high scores for SaaS, uniform near-zero scores for the Indonesian platforms) is far higher and would raise kappa substantially. Second, the disagreements were overwhelmingly of one point in either direction, and they fell within typological categories, not across them. The headline finding, the six-point jurisdictional gap visible in Figure 3, is therefore unlikely to be an artifact of the disagreements observed, although only ten platforms were re-coded. It turns on the contrast between clusters on which the coders agreed, not on the contested cells that separate them.

3.5 Effect sizes, robustness and construct validity

The jurisdictional contrast is large, not merely significant. The rank-biserial correlation for the GDPR-versus-local comparison is r = 0.88, which indicates almost complete separation of the two distributions seen in Figure 3 (panel A). The business-model comparison yields a trivial difference (0.17 points on a ten-point scale). A non-significant difference of 0.17 points between groups of this size does not by itself show the absence of an effect. The sector analysis (p = 0.14) is treated as exploratory, since it is underpowered across seven small cells. Three checks support the instrument's validity. Per-indicator reliability shows disagreement concentrated in F1, F9 and F10, and near-perfect agreement for the disclosure and choice indicators F4, F7 and F8. Re-running the headline contrast under the adversarial coder's codes is reported to leave the six-point gap essentially unchanged. The index also shows criterion validity against authoritative legal determinations: platforms that were the subject of adverse regulatory findings (Google, via the CNIL; the IAB Europe TCF, via the Belgian DPA) score low on the same indicators those decisions targeted before remediation, and higher afterward.[32,43,49]

4. Discussion

4.1 Free consent as legal fiction: reading the results against the doctrine

The central result is simple: free consent, the doctrinal cornerstone of consent-based data protection, is empirically the exception rather than the rule. Fewer than half of the platforms studied obtain consent through an interface that offers a real, symmetric, unbundled and non-deceptive choice. The majority manufacture assent, whether by steering it, coercing

it, or dispensing with the consent moment altogether. Read against the interpreted text of Article 4(11) GDPR, this is no marginal shortfall. It is a failure of the operative condition. Consent given through a pre-ticked box is not valid under *Planet49*, and consent nudged by design falls, on the EDPB's reading in Guidelines 03/2022, short of the 'freely given' standard, and consent presumed from mere use is not an 'unambiguous indication' given by a 'clear affirmative action' at all. The grammatical, systematic and teleological readings converge on one conclusion. For a majority of the interfaces examined, the click signifies nothing the doctrine assumes it to signify [3].

4.2 The Brussels effect is enforcement-contingent

The cross-jurisdictional pattern in Figure 3 is compatible with enforcement risk as a cause. Business model does not predict consent quality, but jurisdiction overwhelmingly does. The compliant flows are also disproportionately those an enforcer has already punished. Together these facts suggest that the quality of digital consent depends not on the drafter's good faith but on the credible threat of enforcement in the place where the user can complain [10]. That is a bleak gloss on the Brussels-effect thesis. The GDPR's standards do diffuse, since the China-origin platforms exposed to EU enforcement carry them, but they follow the contour of enforcement risk, not the contour of the firm's global footprint. Where a platform judges that a class of users cannot effectively complain, as may be the case with the Indonesian and regional services here, the consent interface may collapse to a bundled clause or disappear entirely [8]. The pattern suggests that protection may be geo-tailored to the regulator rather than to the user. This finding qualifies the optimistic reading of legal diffusion and re-centers enforcement capacity as the operative variable.

The literature on the Brussels effect gives this reading a frame. Bradford argues that the European Union exports its rules through market mechanisms, because a large firm often finds one strict standard cheaper than many local ones.[36] The mechanism needs a regulator that can credibly threaten sanctions. Japan's data law shows growing EU influence, while Singapore's has stayed comparatively insulated and driven mainly by competition,[50] and a comparison of Vietnam, Indonesia, Malaysia and Singapore finds convergence on concepts but divergence in enforcement.[51] Measurements of banners tell a mixed story about what enforcement achieves. Work on the emergence of consent management tied the adoption of consent-management platforms to uncertainty about sanctions after the GDPR took effect,[47] whereas a 31-country audit finds only 15% of consent interfaces minimally compliant, with compliance varying by country and by platform, and little evidence that guidance and fines raised it.[9] A crawl of sites in 18 countries found that websites largely applied one notice standard to all visitors, whatever their location, and that the site's top-level domain explained much of the variation.[52] That is a reason to treat geo-tailoring as a hypothesis. Taken together, these studies support a cautious version of the enforcement reading: enforcement probably matters, but the size of its effect is contested, and the six-point gap in this sample is best read as a description, not as an estimate of a causal effect.

4.3 Comparative analysis: the EU, Indonesia and Singapore

A functional comparison across the three regimes governing the sample clarifies the mechanism and is summarized in Table 3. On the definitional dimension the three converge. The GDPR (Art. 4(11)), the UU PDP (Arts 20–22) and the Singapore PDPA all require a consent that is informed and purpose-specific, and all treat bundled or coerced consent as suspect. The divergence lies not in the black-letter standard but in its enforcement architecture and its realization in practice. In the EU, a network of well-resourced supervisory authorities, armed with turnover-based fines and a body of banner-level jurisprudence, has made non-compliance costly enough to move interfaces. Singapore's PDPC has built a credible, if less punitive, enforcement record through published decisions.[53] Indonesia is different. There the standard is, on paper, of GDPR pedigree, but the supervisory institution contemplated by Articles 58–60 UU PDP was not yet fully constituted at the time of coding, and no banner-level enforcement had occurred; the transition period under Article 74 had only just expired in October 2024.[13,54] The comparative lesson is plain. Convergence at the level of the rule coexists with radical divergence at the level of the remedy, and the comparison in Table 3 suggests that the remedy matters. As to legal transplantation,[55,56] moving the GDPR's consent standard without moving its enforcement apparatus yields the standard's form without its function, the outcome visible in the Indonesian illusory-consent cluster.

Table 3. Functional comparison of the consent regimes governing the sample.

Dimension	European Union (GDPR)	Indonesia (UU PDP)	Singapore (PDPA)
Consent definition	Freely given, specific, informed, unambiguous (Art. 4(11))	Explicit, valid, purpose-specific (Arts 20–22)	Informed, purpose-limited consent
Anti-coercion rule	Art. 7(4): bundling/wall presumptively invalid	Arts 20–22: valid-consent conditions	Consent obligation; deemed-consent limits
Supervisory body	Independent DPAs, turnover-based fines	Authority under Arts 58–60 (not yet fully operational)	PDPC — active enforcement
Interface enforcement	Banner-level fines and jurisprudence (CNIL; BE-DPA)	None at banner level to date	Moderate; guidance-led
Observed FCI (this study)	8.12 (GDPR-tier flows)	1.75 (local flows)	Regional benchmark

Note. GDPR = General Data Protection Regulation; UU PDP = *Undang-Undang Pelindungan Data Pribadi*; PDPA = Personal Data Protection Act; PDPC = Personal Data Protection Commission; DPA = data-protection authority; FCI = Free Consent Index.

4.4 Implications for Indonesia and the limits of the consent paradigm

For Indonesia the implication is immediate and uncomfortable. The UU PDP imports a GDPR-style consent standard and entered its enforcement phase in October 2024. Yet the domestic platforms on which most Indonesians transact daily (the marketplaces, news sites and e-wallets that occupy the illusory-consent floor of Table 2) fold consent into their terms of use or omit the consent moment altogether. The statute's text is not the binding constraint. What binds is the absence, so far, of the kind of credible, banner-level enforcement that rebuilt Google's and Microsoft's interfaces in Europe [10]. A deeper doctrinal implication follows. If free consent is this fragile and this contingent on enforcement, the wisdom of building data-protection law so heavily on consent at all is in question. The

platforms at the coerced and illusory ends of the spectrum reveal the limits of the consent paradigm: consent that is the price of an indispensable service, or that is presumed from mere use, is autonomy in name only [3]. The evidence lends weight to the scholarly turn toward reducing reliance on consent, through data-minimization duties, purpose limitation enforced independently of consent, and outright prohibitions on the most manipulative design patterns, so that the lawfulness of processing does not rest on a click that so often signifies nothing.[17,57]

The scholarship on consent supplies the doctrinal frame for that doubt. Richards and Hartzog distinguish unwitting, coerced and incapacitated consent and argue that valid consent needs infrequent choices and the right incentives,[58] which echoes the nudged, coerced and illusory types coded here. Solove goes further. He treats consent in privacy law as largely fictional and proposes regulating around the fiction.[3] A relational turn would move the legal focus from individual control to the duties that data holders owe because of their power over individuals.[59] Consent-or-pay models put the question in its sharpest form: is consent free when refusal has a price? Analyses of Meta's pay-or-okay model and of the wider European practice raise concerns under data-protection, consumer and competition law.[60,61] A large-scale measurement of cookie paywalls adds that the 431 paywalls found all relied on the IAB framework and extensively on legitimate interest, which they conflated with consent.[62] Outside the GDPR, the Digital Services Act prohibits deceptive and manipulative interface design in its Article 25, and recent mapping work links 59 known dark patterns to the three autonomy violations that the article names.[63] Interface law is beginning to do some of the work that consent doctrine could not.

4.5 De lege lata assessment and de lege ferenda reform

De lege lata, the evidence exposes three deficiencies in the current Indonesian regime. First, the UU PDP's consent standard is textually adequate but practically unenforced at the interface level. No provision translates the abstract requirement of 'explicit' consent into concrete interface obligations. Second, the supervisory institution required by Articles 58–60 is not yet operational with banner-level audit capacity, so the standard has no credible remedy behind it. Third, the statute still leans on consent as the dominant lawful basis, and it imposes no strong, independently enforced data-minimization duty. Against these gaps, the study grounds three concrete *de lege ferenda* proposals.[13,54]

Recent Indonesian scholarship reaches the same diagnosis from the doctrinal side. Studies of the missing supervisory authority describe a regulatory vacuum, with weak enforcement, lower public trust and legal uncertainty,[64–66] and a study of marketplace applications finds that Indonesian law covers dark patterns only in part.[46] The institutional gap was still open in the 2025 literature reviewed here: the agency of Article 58 UU PDP had not been established, and the authors describe that as the main reason the statute is weakly enforced.[64,66]

(1) Legislative. The Government and the House of Representatives (*Pemerintah and DPR RI*) hold the legislative power under Article 20 of the 1945 Constitution. The Government should issue an implementing government regulation, or the Government and the House should amend the UU PDP, to give the consent standard concrete interface content. It would mandate a symmetric first-layer reject of equal prominence to accept, prohibit pre-selected non-essential processing, and require the unbundling of tracking consent from acceptance of the general terms. The constitutional basis is Article 28G(1) read with Article 28D(1) (legal certainty). The international basis is the GDPR benchmark (Arts 4(11), 7) and the EDPB's deceptive-design guidance, which together supply a ready, tested template.[15,20]

(2) Regulatory. The Ministry of Communication and Digital Affairs, as the sectoral regulator under GR 71/2019, should issue a binding technical standard for consent interfaces of electronic-system operators. A published audit methodology modeled on the Free Consent Index should accompany it, so that compliance is objectively verifiable and non-compliance is documented. The basis is the Ministry's existing supervisory mandate over electronic systems. The rationale: an objective, published metric converts a vague standard into an auditable one and lowers the cost of enforcement [11].

(3) Institutional. The data-protection supervisory authority contemplated by Articles 58–60 UU PDP should be constituted with genuine independence. It needs banner-level audit capacity and the ability to use the administrative fines of up to 2% of annual revenue that Article 57(3) UU PDP already provides, and it should adopt a first enforcement program targeting the highest-traffic domestic marketplaces, news sites and e-wallets, the illusory-consent cluster identified in Table 2. The basis is Articles 58–60 UU PDP. The rationale, drawn directly from the cross-jurisdictional evidence, is simple: a consent standard changes interfaces only once a credible enforcer makes the cost of the illusion exceed the cost of a compliant interface, as occurred in the EU. All three proposals rest constitutionally on Article 28G(1) of the 1945 Constitution, and they fit Indonesia's broader ASEAN and international commitments.[51]

4.6 A phased, authority-anchored reform roadmap

The three reform proposals are not equally urgent. The cross-jurisdictional evidence dictates their sequence. The binding constraint is institutional: a consent standard moves interfaces only once a credible enforcer makes the illusion costlier than compliance, so the constitution of the supervisory authority under Articles 58–60 UU PDP must come first. The regulatory proposal can proceed in parallel under existing legal authority, though. The Ministry of Communication and Digital Affairs may adopt the Free Consent Index as the compliance-audit rubric for electronic-system operators under GR 71/2019 without awaiting new primary legislation, which immediately makes non-compliance objectively documentable and lowers the eventual enforcement cost [11]. The legislative proposal, an implementing regulation or amendment giving the consent standard concrete interface content, can then follow. It would codify the rubric that regulation and enforcement have already validated in practice. This phased design turns an all-or-nothing wish-list into a realistic program. Each stage lowers the cost of the next [42].

4.7 Limitations

Four limitations qualify these claims. First, inter-coder reliability on the contested subsample was moderate (kappa = 0.38). This reflects the deliberate over-sampling of the hardest cases and does not disturb the cluster-level finding. Still, the exact index value for any individual platform in the interpretively contested middle should be read as approximate rather than precise. Second, the coding captures the design of the consent interface as evidenced in policies, live banners and regulatory records. It is not a controlled observation of every flow from every geography. Live EU banners are geo-served, so some first-layer features for platforms observed from outside the EU were coded conservatively from documentation, which will if anything understate a few GDPR-tier scores. Third, the cross-jurisdictional contrast is partly a contrast of platform composition. The local-flow group consists of Indonesian and regional platforms, so the six-point gap conflates the jurisdiction with the particular firms. A within-platform design coding the same global service across geographies would isolate the regulatory effect more cleanly. It is the natural next study. Fourth, the sample of forty is purposive and built for variation. The prevalence figures describe this constructed sample, not the universe of digital services, although the inferential contrasts are internal to it. Fifth, the legal and institutional facts are time-dependent.

The Belgian decision of February 2022 was annulled on procedural grounds and replaced by the Brussels Market Court on 14 May 2025, which confirmed the fine,[30] and the literature reviewed here still describes the Indonesian supervisory agency as not yet established.[64,66] Sixth, the typology shares five indicators with the index, the rule that codes unverifiable features as 0 may widen the gap, and two validity checks rest on a recoding of only ten platforms (Sections 2.4, 2.5 and 3.5). The six-point gap is therefore best read as a descriptive contrast.

5. Conclusion

This article measured the illusion of free consent by coding the consent architecture of forty digital platforms against ten indicators of consent validity (Table 1) and mapping them onto a typology of genuine, nudged, coerced and illusory consent (Table 2). De lege lata, genuine free consent was the exception, present in only 45% of platforms. Most platforms manufactured assent through dark patterns, coercion, or the outright absence of a consent moment. Jurisdictional flow was the variable most strongly associated with the index, and business model was not. GDPR-tier flows scored 8.12 against 1.75 for Indonesian and regional local flows (Figure 3), and even the GDPR flows fell short of the ideal, largely under enforcement compulsion. One interpretation ties these results together. The freedom of digital consent may depend on the credible threat of enforcement in the place where the user can complain, and not on the good faith of the standard-form drafter.

De lege ferenda, the study commends three reforms for Indonesia: a legislative rule giving the UU PDP consent standard concrete interface content; a regulatory technical standard and audit methodology for the Ministry of Communication and Digital Affairs; and the constitution of an independent, adequately empowered supervisory authority to enforce at the banner level. For data-protection law the warning is double. A consent standard on paper will not by itself dislodge the bundled and illusory interfaces that dominate its domestic market. More fundamentally, a legal edifice resting on the fiction of the free click may rest on sand. Future research should extend the design to a within-platform comparison of the same global service across geographies, isolating the enforcement effect still more cleanly.

Declarations

Ethics Approval and Consent

Not applicable. The study analyzed publicly available consent interfaces and legal instruments and involved no human subjects, so ethics committee approval was not required.

Use of Artificial Intelligence

None. No artificial intelligence tools were used to generate, analyze or write any part of this work.

Author Contributions

H.P.: Conceptualization, Methodology, Investigation, Formal analysis, Visualization, Writing – original draft. H.P.P.: Data curation, Validation, Writing – review & editing. F.F.: Supervision, Project administration, Writing – review & editing. All 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.

Data Availability

The coded dataset, coding manual, blind reliability key and analysis script are available from the corresponding author on reasonable request.

Acknowledgments

None. The authors have no individuals or institutions to acknowledge.

References

1. 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.
2. *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.
3. Solove DJ. Murky consent: an approach to the fictions of consent in privacy law. Boston Univ Law Rev. 2024;104(2):593–639.
4. Bongard-Blanchy K, Rossi A, Rivas S, et al. "I am definitely manipulated, even when I am aware of it. It's ridiculous!": dark patterns from the end-user perspective. Proc 2021 ACM Designing Interactive Systems Conf (DIS '21). 2021:763–776. doi:10.1145/3461778.3462086
5. Gray CM, Santos C, Bielova N, Toth M, Clifford D. Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. Proc 2021 CHI Conf Human Factors Comput Syst (CHI '21). 2021:1–18. doi:10.1145/3411764.3445779
6. Mathur A, Kshirsagar M, Mayer J. What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. Proc 2021 CHI Conf Human Factors Comput Syst (CHI '21). 2021:1–18. doi:10.1145/3411764.3445610
7. Krisam C, Dietmann H, Volkamer M, Kulyk O. Dark patterns in the wild: review of cookie disclaimer designs on top 500 German websites. Proc 2021 Eur Symp Usable Secur (EuroUSEC '21). 2021:1–8. doi:10.1145/3481357.3481516
8. Papadogiannakis E, Papadopoulos P, Kourtellis N, et al. User tracking in the post-cookie era: how websites bypass GDPR consent to track users. Proc Web Conf 2021 (WWW '21). 2021:2130–2141. doi:10.1145/3442381.3450056
9. Nouwens M, Kristensen JB, Maalt K, et al. A cross-country analysis of GDPR cookie banners and flexible methods for scraping them. Proc 2025 CHI Conf Hum Factors Comput Syst (CHI '25). 2025:1–28. doi:10.1145/3706598.3713648
10. Kretschmer M, Pennekamp J, Wehrle K. Cookie banners and privacy policies: measuring the impact of the GDPR on the web. ACM Trans Web. 2021;15(4):1–42. doi:10.1145/3466722
11. Bouhoula A, Kubicek K, Zac A, et al. Automated large-scale analysis of cookie notice compliance. Proc 33rd USENIX Secur Symp (USENIX Security '24). 2024:1723–1739.
12. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945* [1945 Constitution of the Republic of Indonesia], Articles 20, 28D(1) and 28G(1).
13. Syailendra MR, Lie G, Sudiro A. Personal data protection law in Indonesia: challenges and opportunities. Indones Law Rev. 2024;14(2):193–210. doi:10.15742/ilrev.v14n2.4
14. Shahrullah RS, Park J, Irwansyah I. Examining personal data protection law of Indonesia and South Korea: the privacy rights fulfilment. Hasanuddin Law Rev. 2024;10(1):1–20. doi:10.20956/halrev.v10i1.5016
15. Santos C, Bielova N, Matte C. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Technol Regul. 2020;2020:91–135. doi:10.71265/g317tv72
16. Nouwens M, Liccardi I, Veale M, et al. Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. Proc 2020 CHI Conf Hum Factors Comput Syst (CHI '20). 2020:1–13. doi:10.1145/3313831.3376321
17. Gray CM, Sanchez Chamorro L, Obi I, et al. Mapping the landscape of dark patterns scholarship: a systematic literature review. Companion Publ 2023 ACM Des Interact Syst Conf (DIS '23 Companion). 2023:188–193. doi:10.1145/3563703.3596635
18. Court of Justice of the European Union. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH*. Case C-673/17. ECLI:EU:C:2019:801. Judgment of 1 October 2019.
19. European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted 4 May 2020.
20. European Data Protection Board. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0. Adopted 14 February 2023.

21. Toth M, Bielova N, Roca V. On dark patterns and manipulation of website publishers by CMPs. Proc Priv Enhanc Technol. 2022;2022(3):478–497. doi:10.56553/popets-2022-0082
22. Mathur A, Acar G, Friedman MJ, et al. Dark patterns at scale: findings from a crawl of 11K shopping websites. Proc ACM Hum-Comput Interact. 2019;3(CSCW):1–32. doi:10.1145/3359183
23. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2021-023 du 31 décembre 2021 *concernant les sociétés* Google LLC et Google Ireland Limited.
24. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2021-024 du 31 décembre 2021 *concernant la société* Facebook Ireland Limited.
25. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2022-027 du 29 décembre 2022 *concernant les sociétés* TikTok.
26. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2022-023 du 19 décembre 2022 *concernant la société* Microsoft Ireland Operations Limited.
27. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2020-012 du 7 décembre 2020 *concernant les sociétés* Google LLC et Google Ireland Limited.
28. Commission Nationale de l'Informatique et des Libertés. *Délibération de la formation restreinte* no. SAN-2020-013 du 7 décembre 2020 *concernant la société* Amazon Europe Core.
29. Belgian Data Protection Authority (Litigation Chamber). Decision on the merits 21/2022 of 2 February 2022 concerning IAB Europe (case DOS-2019-01377). Annulled on procedural grounds and replaced by a judgment of the Brussels Market Court of 14 May 2025.
30. Belgian Data Protection Authority. The Market Court rules in the IAB Europe case [Internet]. Brussels: Belgian Data Protection Authority; 2025. Available from: https://www.dataprotectionauthority.be/the-market-court-rules-in-the-iab-europe-case
31. European Data Protection Board. Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms. Adopted 17 April 2024.
32. Veale M, Nouwens M, Santos C. Impossible asks: can the Transparency and Consent Framework ever authorise real-time bidding after the Belgian DPA decision? Technol Regul. 2022;2022:12–22. doi:10.71265/0ccteg67
33. Utz C, Degeling M, Fahl S, et al. (Un)informed consent: studying GDPR consent notices in the field. Proc 2019 ACM SIGSAC Conf Comput Commun Secur (CCS '19). 2019:973–990. doi:10.1145/3319535.3354212
34. Habib H, Li M, Young E, et al. "Okay, whatever": an evaluation of cookie consent interfaces. Proc 2022 CHI Conf Hum Factors Comput Syst. 2022:1–27. doi:10.1145/3491102.3501985
35. Berens BM, Bohlender M, Dietmann H, et al. Cookie disclaimers: dark patterns and lack of transparency. Comput Secur. 2024;136:103507. doi:10.1016/j.cose.2023.103507
36. Bradford A. The Brussels effect: how the European Union rules the world. New York: Oxford University Press; 2020. doi:10.1093/oso/9780190088583.001.0001
37. Soe T, Nordberg O, Guribye F, et al. Circumvention by design: dark patterns in cookie consent for online news outlets. Proc 11th Nordic Conf Hum-Comput Interact (NordiCHI '20). 2020:1–12. doi:10.1145/3419249.3420132
38. Court of Justice of the European Union. *Meta Platforms Inc and Others v Bundeskartellamt*. Case C-252/21. ECLI:EU:C:2023:537. Judgment of 4 July 2023.
39. Parliament of Singapore. Personal Data Protection Act 2012 (Act 26 of 2012).
40. *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik* [Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions]. *Lembaran Negara Republik Indonesia* Tahun 2019 Nomor 185, *Tambahan Lembaran Negara* Nomor 6400.
41. Santos C, Nouwens M, Toth M, et al. Consent management platforms under the GDPR: processors and/or controllers? Priv Technol Policy (APF 2021). Lect Notes Comput Sci. 2021;12703:47–69. doi:10.1007/978-3-030-76663-4_3
42. Gunawan J, Pradeep A, Choffnes D, et al. A comparative study of dark patterns across web and mobile modalities. Proc ACM Hum-Comput Interact. 2021;5(CSCW2):1–29. doi:10.1145/3479521
43. Bollinger D, Kubicek K, Cotrini C, et al. Automating cookie consent and GDPR violation detection. Proc 31st USENIX Secur Symp (USENIX Security '22). 2022:2893–2910.
44. Kyi L, Ammanaghatta Shivakumar S, Santos C, et al. Investigating deceptive design in GDPR's legitimate interest. Proc 2023 CHI Conf Hum Factors Comput Syst (CHI '23). 2023:1–16. doi:10.1145/3544548.3580637
45. Rasaii A, Gosain D, Gasser O. Thou shalt not reject: analyzing accept-or-pay cookie banners on the web. Proc 2023 ACM Internet Meas Conf (IMC '23). 2023:154–161. doi:10.1145/3618257.3624846
46. Annisa A, Hutabarat SMD. Legal protection for consumers in the context of dark patterns in Indonesian marketplace applications: a comparative study with the Netherlands. Rechtsidee. 2026;14(1). doi:10.21070/jihr.v14i1.1149
47. Hils M, Woods DW, Böhme R. Measuring the emergence of consent management on the web. Proc ACM Internet Meas Conf (IMC '20). 2020:317–332. doi:10.1145/3419394.3423647
48. Morel V, Santos C, Lintao Y, et al. Your consent is worth 75 euros a year: measurement and lawfulness of cookie paywalls. Proc 21st Workshop Priv Electron Soc (WPES '22). 2022:213–218. doi:10.1145/3559613.3563205
49. 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. 2020 IEEE Symp Secur Priv (SP). 2020:791–809. doi:10.1109/sp40000.2020.00076
50. Zhang D. The EU's digital footprint: shaping data governance in Japan and Singapore. Polit Gov. 2025;13. doi:10.17645/pag.10422
51. 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. doi:10.69554/jyui7132
52. van Eijk R, Asghari H, Winter P, et al. The impact of user location on cookie notices (inside and outside of the European Union). arXiv [preprint]. 2021:2110.09832. doi:10.48550/arXiv.2110.09832
53. Lim S. Cybersecurity and data protection: some empirical observations, and a lacuna in the PDPA? SSRN [preprint]. 2021. doi:10.2139/ssrn.3951721
54. 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
55. Teubner G. Legal irritants: good faith in British law or how unifying law ends up in new divergencies. Mod Law Rev. 1998;61(1):11–32. doi:10.1111/1468-2230.00125
56. 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
57. Schermer BW, Custers B, van der Hof S. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. Ethics Inf Technol. 2014;16:171–182. doi:10.1007/s10676-014-9343-8
58. Richards N, Hartzog W. The pathologies of digital consent. Wash Univ Law Rev. 2019;96(6):1461–1503.
59. Richards N, Hartzog W. A relational turn for data protection? Eur Data Prot Law Rev. 2020;6(4):492–497. doi:10.21552/edpl/2020/4/5
60. D'Amico A, Pelekis D, Teixeira Santos C, et al. Meta's pay-or-okay model: an analysis under EU data protection, consumer and competition law. Technol Regul. 2024;2024:254–272. doi:10.71265/tkk29041
61. Yücedağ N, Akkanat Öztürk EB, Aşıkoğlu SI. Pay or consent models in Europe: already outdated or an overlooked crisis in freely given consent? Technol Regul. 2025;2025:336–354. doi:10.71265/8jjzhc21
62. Morel V, Santos C, Fredholm V, et al. Legitimate interest is the new consent: large-scale measurement and legal compliance of IAB Europe TCF paywalls. Proc 22nd Workshop Priv Electron Soc (WPES '23). 2023:153–158. doi:10.1145/3603216.3624966
63. Ahuja S, Gunawan J, Bielova N, et al. Dark patterns and the EU Digital Services Act: mapping autonomy violations and design factors. Proc 2026 CHI Conf Hum Factors Comput Syst (CHI '26). 2026:1–30. doi:10.1145/3772318.3791479
64. 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
65. Neta Y, Awanisa A, Melisa M. The urgency of establishing independent supervisory authority for personal data protection in Indonesia. Constitutionale. 2022;3(1):19–38. doi:10.25041/constitutionale.v3i1.2535
66. Hernowo BA. The challenges of implementing the Personal Data Protection Law in Indonesia: delays in establishing a regulatory authority. Proc First Int Cyber Law Conf (ICL-C 2023). 2025. doi:10.4108/eai.11-11-2023.2351333