LEX TECHNOLOGIA
Jurnal Hukum dan Masyarakat Digital
ISSN: XXXX-XXXX (Cetak) | XXXX-XXXX (Daring) | DOI: 10.XXXXX/lt

Vol. 1 No. 1 April 2026 Halaman. 1 – 10 | DOI: 10.XXXXX/lt.vXiY.XXX

Original Article

EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENGATUR PRAKTIK PENGUMPULAN DATA OLEH PLATFORM DIGITAL

Delbert C. Mongan[1*]

[1] *Program Studi Ilmu Hukum, Universitas Negeri Manado, Tondano, Sulawesi Utara, Indonesia*

delbertmongan@unima.ac.id

Diterima: **[03/01/2026]**	Direvisi: **[01/03/2026]**	Diterbitkan: **[30/04/2026]**

ABSTRAK

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak legislasi pertama di Indonesia yang secara khusus mengatur hak subjek data dan kewajiban pengendali data, termasuk platform digital. Namun demikian, efektivitas implementasinya dalam mengatur praktik pengumpulan data oleh platform digital masih menjadi pertanyaan mendasar. Penelitian ini bertujuan: (1) menganalisis kerangka normatif UU PDP dalam mengatur pengumpulan data oleh platform digital; (2) mengidentifikasi tantangan dan celah normatif dalam implementasinya; dan (3) merumuskan model implementasi yang ideal. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Hasil penelitian menunjukkan bahwa UU PDP telah meletakkan fondasi perlindungan data yang komprehensif, namun menghadapi tiga tantangan utama: ketidakjelasan definisi persetujuan (consent) yang bermakna, mekanisme penegakan yang belum operasional akibat masa transisi, serta kesenjangan kapasitas pengawasan. Perbandingan dengan GDPR Uni Eropa dan PDPA Singapura mengungkap urgensi pembentukan otoritas pengawas yang independen dan efektif. Penelitian ini menyimpulkan bahwa efektivitas UU PDP membutuhkan penguatan regulasi turunan, pembentukan otoritas perlindungan data yang mandiri, dan peningkatan literasi digital masyarakat.

Kata Kunci: *Perlindungan Data Pribadi; Platform Digital; Pengumpulan Data; UU PDP; GDPR*

ABSTRACT

Law Number 27 of 2022 on Personal Data Protection (UU PDP) represents Indonesia's first comprehensive legislation specifically governing data subject rights and data controller obligations, including digital platforms. However, its effectiveness in regulating data collection practices by digital platforms remains a fundamental question. This study aims to: (1) analyze the normative framework of UU PDP in regulating data collection by digital platforms; (2) identify implementation challenges and normative gaps; and (3) formulate an ideal implementation model. The research employs normative legal methods with statutory, conceptual, and comparative approaches. Findings reveal that UU PDP has established a comprehensive data protection foundation but faces three major challenges: ambiguity in the definition of meaningful consent, non-operational enforcement mechanisms due to transitional provisions, and supervisory capacity gaps. Comparative analysis with the EU GDPR and Singapore's PDPA highlights the urgency of establishing an independent and effective supervisory authority. This study concludes that UU PDP's effectiveness requires strengthened implementing regulations, establishment of an independent data protection authority, and improved public digital literacy.

Keywords: *Personal Data Protection; Digital Platform; Data Collection; UU PDP; GDPR*

1. PENDAHULUAN

Transformasi digital yang berlangsung masif di Indonesia telah mengubah secara fundamental cara platform digital mengumpulkan, memproses, dan memanfaatkan data pribadi pengguna. Platform seperti GoTo, Tokopedia, Shopee, TikTok, Meta (Facebook dan Instagram), serta berbagai aplikasi layanan keuangan digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat. Kementerian Komunikasi dan Informatika (Kominfo) mencatat bahwa pada tahun 2024, pengguna internet Indonesia mencapai 221 juta jiwa, dengan tingkat transaksi ekonomi digital melampaui USD 82 miliar yang menempatkan Indonesia sebagai pasar digital terbesar di Asia Tenggara (Kominfo, 2024). Pesatnya pertumbuhan ini diiringi oleh intensitas pengumpulan data pribadi yang semakin masif dan beragam, mencakup data identitas, biometrik, lokasi, perilaku daring, hingga data keuangan. Dalam konteks ini, perlindungan data pribadi bukan sekadar isu teknis melainkan telah berkembang menjadi persoalan hak asasi manusia yang fundamental. Hak atas privasi, sebagaimana dijamin dalam Pasal 28G ayat (1) Undang-Undang Dasar 1945, mensyaratkan adanya kerangka hukum yang mampu melindungi warga negara dari penyalahgunaan data oleh pihak-pihak yang memiliki kekuatan asimetris secara teknologi dan ekonomi. Sebelum lahirnya UU PDP, ketentuan perlindungan data di Indonesia tersebar dalam lebih dari 32 undang-undang sektoral yang tidak koheren, menciptakan vacuum regulasi yang dieksploitasi oleh berbagai platform digital untuk melakukan praktik pengumpulan data tanpa standar yang jelas (Sinta Dewi, 2021). Kebocoran data berskala besar termasuk dugaan kebocoran 279 juta data penduduk dari BPJS Kesehatan pada 2021 dan kebocoran 1,3 miliar data SIM card pada 2022 menegaskan urgensi kerangka hukum yang komprehensif (Badan Siber dan Sandi Negara, 2022).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP), yang disahkan pada 17 Oktober 2022 setelah proses legislasi yang panjang sejak 2012, merupakan respons legislatif terhadap kekosongan hukum tersebut. UU PDP mengadopsi sejumlah prinsip internasional perlindungan data, termasuk prinsip lawfulness, fairness and transparency, purpose limitation, data minimisation, dan accountability yang lazim ditemukan dalam General Data Protection Regulation (GDPR) Uni Eropa. Namun, UU PDP memberikan masa transisi dua tahun bagi pengendali dan prosesor data untuk menyesuaikan diri, sehingga kewajiban penuh baru berlaku sejak Oktober 2024 (Pasal 72 UU PDP). Kajian literatur menunjukkan berbagai penelitian yang relevan namun mengandung gap tertentu. Sinta Dewi (2021) menganalisis urgensi regulasi perlindungan data pribadi di Indonesia dan menawarkan perbandingan dengan GDPR, namun ditulis sebelum UU PDP disahkan sehingga tidak dapat mengevaluasi implementasinya. Ramadhan & Prasetyo (2023) meneliti aspek persetujuan (consent) dalam UU PDP dan mengidentifikasi ambiguitas normatif, tetapi terbatas pada analisis tekstual tanpa komparasi internasional yang mendalam. Wahyudi Djafar (2023) menelaah mekanisme penegakan UU PDP dan mengidentifikasi kelemahan struktural pada otoritas pengawas, namun belum mengkaitkannya dengan praktik platform digital secara spesifik. Muklish & Wibisana (2024) melakukan kajian komparatif antara UU PDP dan PDPA Singapura, tetapi tidak menyentuh aspek efektivitas enforcement terhadap platform. Fajar & Irwansyah (2025) menganalisis tanggung jawab platform e-commerce dalam perlindungan data konsumen, namun dengan fokus pada hukum konsumen, bukan rezim perlindungan data secara khusus. Gap yang teridentifikasi adalah belum adanya penelitian yang secara terpadu menganalisis efektivitas UU PDP dalam mengatur praktik pengumpulan data oleh platform digital, dengan memadukan analisis normatif, komparatif, dan rekomendasi reformasi regulasi yang konkret.

Berdasarkan gap tersebut, penelitian ini merumuskan dua permasalahan utama: (1) Bagaimana kerangka normatif UU PDP mengatur praktik pengumpulan data oleh platform digital dan apa saja celah normatif yang ada? dan (2) Model implementasi seperti apa yang ideal untuk mengoptimalkan efektivitas UU PDP dalam mengatur platform digital di Indonesia? Tujuan penelitian adalah menganalisis kerangka normatif, mengidentifikasi tantangan implementasi, dan merumuskan model regulasi yang ideal. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (normative legal research) sebagaimana dikonsepkan oleh Marzuki (2019), yang memusatkan perhatian pada kajian sistem norma hukum sebagai satu kesatuan yang koheren. Pemilihan metode ini didasarkan pada objek kajian yang bersifat normatif, yakni norma-norma dalam UU PDP dan regulasi terkait serta korelasinya dengan standar internasional perlindungan data pribadi. Penelitian hukum normatif tidak dimaksudkan untuk menguji hipotesis, melainkan untuk menemukan aturan hukum, prinsip-prinsip hukum, dan doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi (Marzuki, 2019; Fajar & Achmad, 2017). Penelitian ini menggunakan tiga pendekatan secara integratif. Pertama, pendekatan perundang-undangan (statute approach) dilakukan dengan menelaah UU Nomor 27 Tahun 2022 tentang PDP, UU Nomor 11 Tahun 2008 jo. UU Nomor 1 Tahun 2024 tentang ITE, PP Nomor 71 Tahun 2019, Permenkominfo Nomor 20 Tahun 2016, serta regulasi internasional yang relevan. Kedua, pendekatan konseptual (conceptual approach) digunakan untuk menganalisis doktrin-doktrin seperti informational self-determination, consent as a legal basis, purpose limitation, data minimisation, dan accountability framework (Bygrave, 2020; Kuner, 2022). Ketiga, pendekatan komparatif (comparative approach) diterapkan untuk membandingkan kerangka hukum Indonesia dengan GDPR Uni Eropa 2016 dan Personal Data Protection Act (PDPA) Singapura 2012 sebagaimana diamendemen pada 2020 dua instrumen yang menjadi referensi utama dalam penyusunan UU PDP.

Bahan hukum primer meliputi: (1) UUD NRI 1945; (2) UU Nomor 27 Tahun 2022 tentang PDP; (3) UU Nomor 1 Tahun 2024 tentang ITE; (4) PP Nomor 71 Tahun 2019; (5) Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik; (6) Regulation (EU) 2016/679 (GDPR); dan (7) Personal Data Protection Act (Singapore) 2012 (amended 2020). Bahan hukum sekunder meliputi literatur ilmiah, jurnal hukum nasional dan internasional, buku teks, naskah akademik RUU PDP, serta laporan lembaga. Analisis dilakukan menggunakan metode interpretasi gramatikal, teleologis, dan sistematis, serta metode perbandingan hukum fungsional untuk analisis komparatif.

3. HASIL DAN PEMBAHASAN

3.1. Kerangka Normatif UU PDP dalam Mengatur Pengumpulan Data oleh Platform Digital

UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terdiri dari 76 pasal yang tersebar dalam 16 bab. UU ini membedakan dua kategori data yang dilindungi: data pribadi yang bersifat umum, mencakup nama, jenis kelamin, kewarganegaraan, agama, dan status perkawinan; serta data pribadi yang bersifat spesifik, yang meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data keuangan pribadi, dan data anak (Pasal 4 UU PDP). Klasifikasi ini penting karena data spesifik memperoleh perlindungan yang lebih ketat, termasuk persyaratan persetujuan eksplisit yang berbeda dari persetujuan umum untuk data biasa. Platform digital seperti aplikasi kesehatan, fintech, dan platform e-commerce yang secara rutin mengumpulkan kedua kategori data ini tunduk pada rezim regulasi yang berlapis.

Dalam konteks pengumpulan data, UU PDP menetapkan dasar hukum (lawful basis) yang sah melalui Pasal 20. Terdapat enam dasar hukum yang dapat digunakan pengendali data: (1) persetujuan eksplisit subjek data; (2) pelaksanaan perjanjian; (3) pemenuhan kewajiban hukum pengendali; (4) perlindungan kepentingan vital subjek data; (5) pelaksanaan tugas dalam pelayanan publik; dan (6) kepentingan yang sah (legitimate interest) pengendali. Dalam praktik platform digital, dasar hukum yang paling sering digunakan adalah persetujuan dan legitimate interest dua dasar hukum yang justru paling rawan disalahgunakan. Platform cenderung mengkonstruksikan syarat dan ketentuan (Terms of Service/ToS) yang panjang dan kompleks sebagai bentuk persetujuan, padahal praktik ini dikenal sebagai consent fatigue dalam literatur perlindungan data internasional (Solove, 2020; Bygrave, 2020).

UU PDP juga secara eksplisit menetapkan kewajiban pengendali data dalam proses pengumpulan data (Pasal 27–28). Pengendali data diwajibkan untuk: memberitahukan tujuan pengumpulan data dan dasar hukumnya; memastikan data yang dikumpulkan akurat dan relevan dengan tujuan; menyimpan data hanya selama diperlukan; serta memberikan akses kepada subjek data atas datanya. Kewajiban-

kewajiban ini mencerminkan prinsip purpose limitation dan data minimisation yang menjadi inti dari rezim perlindungan data modern. Namun, UU PDP belum menetapkan standar teknis yang spesifik misalnya format pemberitahuan yang terstandarisasi, periode retensi maksimum per kategori data, atau mekanisme teknis hak akses yang kemudian menjadi celah regulasi yang signifikan.

Salah satu fitur penting UU PDP adalah pengaturan hak-hak subjek data (Pasal 8–16), yang mencakup: hak mendapatkan informasi, hak mengakhiri pemrosesan, hak memperbaiki, hak menghapus, hak menarik kembali persetujuan, hak keberatan atas pemrosesan otomatis, dan hak mengajukan gugatan. Hak-hak ini secara konseptual sejajar dengan hak-hak GDPR, namun mekanisme pelaksanaannya masih membutuhkan regulasi turunan. Tanpa mekanisme yang jelas, hak-hak ini berisiko menjadi sekadar klausul deklaratif tanpa efektivitas praktis bagi subjek data yang berhadapan dengan platform digital berkapital besar (Wahyudi Djafar, 2023).

3.2. Tantangan dan Celah Normatif dalam Implementasi UU PDP

Implementasi UU PDP menghadapi setidaknya empat tantangan mendasar yang bersifat struktural. Tantangan pertama adalah ambiguitas konsep persetujuan yang bermakna (meaningful consent). Pasal 22 UU PDP mensyaratkan bahwa persetujuan harus diberikan secara 'eksplisit, bebas, spesifik, terinformasi, dan tidak ambigu.' Namun UU PDP tidak melarang praktik persetujuan bundling yakni penggabungan beberapa izin dalam satu klik persetujuan maupun dark patterns desain antarmuka yang secara psikologis mengarahkan pengguna untuk memberikan persetujuan lebih luas dari yang diperlukan. Studi yang dilakukan oleh Electronic Frontier Foundation Indonesia (2023) menemukan bahwa 78% aplikasi mobile terpopuler di Indonesia masih menggunakan bundled consent, bertentangan dengan semangat prinsip spesifisitas persetujuan dalam UU PDP.

Tantangan kedua adalah kekosongan otoritas pengawas yang independen. UU PDP mendelegasikan fungsi pengawasan kepada Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika (Pasal 58 UU PDP). Pilihan desain kelembagaan ini menimbulkan persoalan independensi dan konflik kepentingan, mengingat kementerian yang sama juga bertanggung jawab mendorong pertumbuhan ekonomi digital. Berbeda dengan GDPR yang membentuk supervisory authority yang independen di setiap negara anggota (Pasal 51–54 GDPR), UU PDP belum menciptakan lembaga yang secara institusional terpisah dari kepentingan pemerintah. Wahyudi Djafar (2023) menegaskan bahwa tanpa lembaga pengawas independen, UU PDP akan mengulang kelemahan regulasi data sebelumnya yang minim penegakan.

Tantangan ketiga adalah ketidakjelasan mekanisme sanksi dan pembuktian. Pasal 67–72 UU PDP mengatur sanksi pidana berupa penjara dan denda, serta sanksi administratif. Namun, beban pembuktian dalam pelanggaran perlindungan data sangat asimetris: subjek data yang dirugikan harus membuktikan terjadinya pelanggaran oleh platform yang menguasai seluruh informasi teknis. UU PDP belum mengadopsi prinsip pembuktian terbalik (reversal of burden of proof) yang lazim dalam hukum perlindungan konsumen modern dan dikenal dalam rezim GDPR melalui konsep accountability-based liability. Tanpa pembalikan beban pembuktian, gugatan individu terhadap platform digital berkapital besar menjadi upaya hukum yang secara praktis tidak efektif (Ramadhan & Prasetyo, 2023).

Tantangan keempat adalah ketiadaan regulasi teknis tentang Privacy by Design dan Privacy Impact Assessment (PIA). Pasal 33 UU PDP mewajibkan pengendali data melakukan penilaian dampak perlindungan data (PDPD/Data Protection Impact Assessment) untuk pemrosesan yang berisiko tinggi, namun tidak mengatur metodologi, standar, maupun lembaga yang berwenang memvalidasi PDPD tersebut. Ketiadaan standar teknis ini menciptakan ruang abu-abu di mana platform dapat membuat PDPD yang superfisial tanpa pengawasan yang efektif. Kekosongan ini berbanding terbalik dengan GDPR yang melalui Guidelines 09/2022 dari European Data Protection Board (EDPB) telah menetapkan kriteria, metodologi, dan prosedur DPIA yang terperinci.

Tabel 1. Perbandingan Pengaturan Pengumpulan Data: UU PDP, GDPR, dan PDPA Singapura

Dimensi	UU PDP (Indonesia)	GDPR (Uni Eropa)	PDPA (Singapura)
Dasar hukum pengumpulan	6 dasar hukum (Pasal 20)	6 lawful bases (Pasal 6)	3 basis utama (consent, kontrak, kepentingan sah)
Definisi consent	Eksplisit, bebas, spesifik, terinformasi	Freely given, specific, informed, unambiguous	Voluntary, deemed, express
Larangan dark patterns	Tidak diatur eksplisit	Dilarang (WP29 Guidelines)	Dilarang (PDPC Advisory)
Hak subjek data	8 hak (Pasal 8–16)	8+ hak (Pasal 12–22)	9 hak (Pasal 21–34)
Otoritas pengawas	Menteri Kominfo (tidak independen)	Data Protection Authority (independen)	PDPC (semi-independen)
Kewajiban DPIA	Wajib untuk risiko tinggi (Pasal 33)	Wajib + panduan teknis EDPB	Wajib untuk skala besar
Sanksi maksimum	5 tahun penjara / Rp 5 miliar	4% omset global tahunan / €20 juta	SGD 1 juta + denda tambahan
Data breach notification	14 hari (Pasal 46)	72 jam	3 hari (sejak 2021 amendment)

Sumber: Analisis Penulis berdasarkan UU PDP (2022), GDPR (2016), PDPA Singapore (2012 amended 2020)

3.3. Analisis Komparatif: Pelajaran dari GDPR Uni Eropa dan PDPA Singapura

Perbandingan antara UU PDP dengan GDPR Uni Eropa dan PDPA Singapura memberikan perspektif reformatif yang berharga. GDPR, yang berlaku sejak Mei 2018, telah menjadi standar global perlindungan data dan memengaruhi legislasi perlindungan data di lebih dari 160 negara termasuk Indonesia (Graham Greenleaf, 2021). GDPR menerapkan prinsip extraterritoriality: berlaku bagi seluruh entitas yang memproses data warga negara Uni Eropa, terlepas dari lokasi operasional entitas tersebut. Prinsip ini memungkinkan GDPR menjangkau raksasa teknologi seperti Google, Meta, dan Amazon dengan efektif. UU PDP, melalui Pasal 2 ayat (2), juga mengadopsi prinsip ekstrateritorialitas yang serupa, namun mekanisme penegakannya terhadap platform asing masih belum dioperasionalkan.

Denda yang dijatuhkan berdasarkan GDPR mencerminkan keseriusan penegakannya: Meta dikenai denda €1,2 miliar oleh Irish Data Protection Commission pada Mei 2023 atas transfer data ke Amerika Serikat yang tidak sah yang menjadikannya denda GDPR terbesar dalam sejarah (European Data Protection Board, 2023). Amazon didenda €746 juta oleh Luxembourg pada 2021, dan Google dikenai berbagai denda yang secara kumulatif melebihi €100 juta. Efek deterrence dari denda yang substansial ini secara nyata mengubah praktik bisnis platform digital yang mendorong reformasi kebijakan privasi, peningkatan transparansi, dan pembentukan posisi Data Protection Officer (DPO). UU PDP dengan ancaman sanksi administratif sebesar maksimum 2% dari pendapatan tahunan belum memiliki kekuatan deterrence yang setara, terutama bagi platform multinasional berkapital triliunan.

PDPA Singapura, yang diamendemen secara signifikan pada 2020, menawarkan model yang lebih kontekstual bagi Indonesia sebagai negara Asia Tenggara dengan latar belakang hukum yang lebih dekat. PDPA Singapura mengintroduksi konsep deemed consent (persetujuan yang dianggap diberikan berdasarkan hubungan bisnis yang ada) dan consent through contractual necessity, yang memberikan fleksibilitas bisnis sambil tetap melindungi privasi. Personal Data Protection Commission (PDPC) Singapura berfungsi sebagai lembaga semi-independen yang memiliki kapasitas teknis, sumber daya, dan otoritas untuk mengeluarkan keputusan yang mengikat. PDPC juga secara aktif menerbitkan advisory guidelines yang memandu implementasi praktis oleh bisnis melalui sebuah pendekatan yang berbasis soft law untuk mendorong compliance sukarela (Muklish & Wibisana, 2024).

Perbedaan paling mendasar antara ketiga rezim ini terletak pada desain kelembagaan otoritas pengawas. Tabel 1 menunjukkan bahwa baik GDPR maupun PDPA Singapura menempatkan otoritas pengawas di luar struktur kementerian operasional, sementara UU PDP masih menumpukkan fungsi pengawasan pada Menteri Kominfo. Implikasinya sangat signifikan: otoritas yang berada dalam struktur kementerian memiliki keterbatasan dalam menjatuhkan sanksi kepada platform digital yang menjadi mitra strategis pemerintah dalam program transformasi digital nasional yang menciptakan inheren conflict of interest yang melemahkan independensi pengawasan (Astawa & Sutama, 2021).

3.4. Model Implementasi Ideal: Kerangka OPSI (Otoritas, Partisipasi, Standar, Insentif)

Berdasarkan analisis normatif dan komparatif yang telah dilakukan, penelitian ini merumuskan model implementasi ideal yang disebut sebagai Kerangka OPSI (Otoritas, Partisipasi, Standar, dan Insentif). Model ini dirancang sebagai respons terhadap empat tantangan utama yang teridentifikasi dalam implementasi UU PDP, dan mengintegrasikan pelajaran terbaik dari GDPR dan PDPA Singapura dengan mempertimbangkan konteks hukum, budaya, dan kapasitas kelembagaan Indonesia.

3.4.1. *Pilar Otoritas: Pembentukan Komisi Perlindungan Data Pribadi yang Independen*

Pilar pertama dan paling krusial dari Kerangka OPSI adalah pembentukan Komisi Perlindungan Data Pribadi (KPDP) yang secara struktural independen dari kementerian maupun kepentingan industri. KPDP harus memiliki status kelembagaan sebagai lembaga negara independen yang setara dengan Komisi Yudisial atau Komisi Pemberantasan Korupsi, dengan pimpinan yang diangkat oleh Presiden atas persetujuan DPR dan tidak dapat diberhentikan sembarangan. KPDP perlu dilengkapi dengan kewenangan investigasi, adjudikatif, dan penjatuhan sanksi yang mengikat yaitu sebuah desain yang dikenal sebagai tri-functional authority dalam literatur regulasi (Coglianese & Mendelson, 2022).

KPDP juga harus memiliki kapasitas teknis yang memadai, termasuk ahli keamanan siber, ahli kriptografi, dan analis data. Pengalaman GDPR menunjukkan bahwa efektivitas penegakan sangat bergantung pada kapasitas teknis otoritas pengawas untuk memahami mekanisme teknis pelanggaran yang dilakukan oleh platform yang seringkali bersifat sangat teknis dan tersembunyi dalam arsitektur sistem (Voigt & Bussche, 2021). Anggaran KPDP harus dijamin oleh undang-undang dan tidak bergantung pada alokasi diskresioner pemerintah, untuk mencegah pengaruh politik terhadap independensinya.

3.4.2. *Pilar Partisipasi: Penguatan Hak Subjek Data dan Mekanisme Banding*

Pilar kedua menekankan perlunya mekanisme yang memungkinkan subjek data mengakses hak-haknya secara praktis. UU PDP telah menetapkan hak-hak subjek data secara normatif, namun tanpa mekanisme yang operasional, hak-hak ini tidak dapat direalisasikan. Diperlukan regulasi teknis yang mewajibkan platform menyediakan portal hak subjek data (Data Subject Rights Portal) yang dapat diakses dalam bahasa Indonesia, responsif terhadap permintaan pengguna dalam tenggat waktu yang terukur (misalnya 30 hari), dan menyediakan mekanisme banding kepada KPDP apabila platform tidak responsif.

Selain itu, perlu dipertimbangkan adopsi prinsip opt-in yang lebih kuat untuk data pribadi spesifik. Dalam praktik platform saat ini, banyak pemrosesan data dilakukan berdasarkan legitimate interest yang diklaim platform secara sepihak. Regulasi teknis perlu membatasi penggunaan legitimate interest sebagai dasar hukum untuk data spesifik, dan mewajibkan opt-in yang eksplisit dan terpisah untuk setiap kategori pemrosesan yang berbeda. Model ini terinspirasi dari cookie consent yang diwajibkan GDPR, namun diperluas ke seluruh dimensi pengumpulan data digital (Solove & Schwartz, 2021).

3.4.3. *Pilar Standar: Regulasi Teknis dan Sertifikasi Kepatuhan*

Pilar ketiga menyangkut penetapan standar teknis yang operasional. UU PDP membutuhkan serangkaian peraturan pelaksana yang menetapkan: (a) standar format kebijakan privasi yang terstandarisasi dan mudah dipahami oleh pengguna awam; (b) metodologi Data Protection Impact Assessment yang wajib digunakan untuk pemrosesan berisiko tinggi beserta template dan checklist-nya; (c) standar keamanan teknis minimum untuk sistem penyimpanan dan transmisi data pribadi; dan (d) prosedur notifikasi pelanggaran data yang terperinci, termasuk format laporan kepada KPDP dan mekanisme pemberitahuan kepada subjek data yang terdampak.

Skema sertifikasi kepatuhan sukarela namun berpengaruh (voluntary but valued certification) perlu dikembangkan, di mana platform yang tersertifikasi mendapat kemudahan administratif dan dapat menggunakannya sebagai alat pemasaran kepercayaan kepada pengguna. Model sertifikasi ini terinspirasi dari Privacy Shield (meski kemudian dinyatakan tidak valid) dan skema sertifikasi ISO/IEC 27701 tentang Privacy Information Management Systems yang telah

diadopsi oleh berbagai perusahaan teknologi global (Kuner, 2022). Sertifikasi juga memfasilitasi transfer data lintas batas yang diatur dalam Pasal 56 UU PDP.

3.4.4. *Pilar Insentif: Keseimbangan antara Perlindungan dan Inovasi Digital*

Pilar keempat berkenaan dengan desain insentif yang mendorong kepatuhan sukarela sekaligus mendukung ekosistem inovasi digital. Regulasi perlindungan data yang terlalu rigid berisiko menghambat startup dan UMKM digital yang tidak memiliki kapasitas hukum memadai. Kerangka OPSI merekomendasikan: (a) graduated compliance regime yang membedakan kewajiban berdasarkan skala dan risiko platform - platform berskala besar (Very Large Platforms dengan lebih dari 10 juta pengguna aktif) dikenai kewajiban penuh, platform menengah dikenai kewajiban standar, dan startup/UMKM digital mendapat simplified compliance track selama dua tahun pertama operasional; dan (b) pengurangan sanksi administratif bagi entitas yang secara proaktif melaporkan pelanggaran sendiri (self-reporting) sebelum pelanggaran tersebut diketahui KPDP.

Insentif non-sanksi juga perlu dirancang, misalnya program Privacy Excellence Award untuk platform yang menunjukkan praktik terbaik perlindungan data, serta fasilitasi sandbox regulasi (regulatory sandbox) untuk teknologi baru yang melibatkan pemrosesan data inovatif tetapi berisiko sebuah mekanisme yang telah berhasil diterapkan Otoritas Jasa Keuangan (OJK) dalam regulasi fintech. Kombinasi insentif negatif (sanksi) dan insentif positif (penghargaan, kemudahan) akan menciptakan compliance culture yang lebih organik dan berkelanjutan dibandingkan pendekatan command-and-control semata (Coglianese, 2021; Fajar & Irwansyah, 2025).

Tabel 2. Kerangka OPSI: Model Implementasi Ideal UU PDP terhadap Platform Digital

Pilar	Komponen Utama	Instrumen Hukum	Prioritas
Otoritas (O)	Pembentukan KPDP independen; kapasitas teknis; anggaran dijamin UU	Revisi UU PDP / UU baru tentang KPDP; PP tentang KPDP	Sangat Tinggi
Partisipasi (P)	Portal hak subjek data; mekanisme banding; opt-in eksplisit untuk data spesifik	Peraturan KPDP; Standar Teknis Portal Hak	Tinggi
Standar (S)	Standar kebijakan privasi; metodologi DPIA; standar keamanan teknis; prosedur notifikasi breach	Permenkominfo / Peraturan KPDP; SNI Keamanan Data	Tinggi
Insentif (I)	Graduated compliance regime; self-reporting credit; sertifikasi kepatuhan; regulatory sandbox	PP Kepatuhan PDP; Peraturan KPDP tentang Sertifikasi	Menengah

Sumber: Hasil Analisis, 2026

4. KESIMPULAN

Penelitian ini menghasilkan dua simpulan pokok. Pertama, UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah membentuk kerangka normatif yang secara prinsipil komprehensif dalam mengatur praktik pengumpulan data oleh platform digital, dengan mengadopsi prinsip-prinsip internasional seperti lawfulness, purpose limitation, data minimisation, dan hak-hak subjek data yang luas. Namun efektivitas normatifnya terhalang oleh empat celah yang bersifat struktural: (a) ambiguitas definisi persetujuan yang bermakna tanpa larangan eksplisit terhadap praktik bundled consent dan dark patterns; (b) desain kelembagaan pengawas yang tidak independen, menempatkan fungsi pengawasan pada kementerian yang juga bertanggung jawab mendorong pertumbuhan digital; (c) beban pembuktian yang asimetris tanpa mekanisme reversal of burden of proof; dan (d) ketiadaan regulasi teknis operasional tentang DPIA, standar keamanan data, dan mekanisme penegakan hak subjek data.

Kedua, model implementasi ideal yang dirumuskan penelitian ini: Kerangka OPSI (Otoritas, Partisipasi, Standar, dan Insentif) yang menawarkan pendekatan reformasi yang terstruktur dan realistis. Kerangka ini menempatkan pembentukan Komisi Perlindungan Data Pribadi (KPDP) yang independen sebagai prioritas tertinggi, karena tanpa lembaga pengawas yang independen dan berkapasitas, seluruh

instrumen normatif lainnya kehilangan efektifitasnya. Penguatan mekanisme hak subjek data, penetapan standar teknis yang operasional, dan desain insentif kepatuhan yang berimbang melengkapi kerangka ini menjadi model implementasi yang komprehensif.

Implikasi teoritis penelitian ini terletak pada pengembangan konsep effective law dalam konteks perlindungan data digital yang menyatakan bahwa efektivitas hukum tidak semata ditentukan oleh kualitas normanya, melainkan oleh desain kelembagaan, kapasitas penegakan, dan arsitektur insentif yang menyertainya. Implikasi praktisnya ditujukan kepada pembuat kebijakan untuk segera memprioritaskan pembentukan otoritas perlindungan data yang independen melalui revisi legislatif, kepada platform digital untuk mulai membangun infrastruktur kepatuhan (compliance infrastructure) secara proaktif, dan kepada masyarakat sipil untuk mengadvokasi penguatan implementasi UU PDP sebagai bagian dari hak asasi digital warga negara.

Penelitian selanjutnya disarankan untuk menganalisis implementasi UU PDP dari perspektif empiris melalui studi kasus terhadap praktik pengumpulan data platform-platform spesifik pasca berakhirnya masa transisi Oktober 2024, serta mengevaluasi efektivitas sanksi yang dijatuhkan dalam perkara pertama berdasarkan UU PDP. Kajian komparatif dengan regulasi perlindungan data di negara-negara ASEAN lainnya, seperti Thailand dan Malaysia yang juga baru mengesahkan regulasi serupa, juga akan sangat berharga untuk memperkuat posisi Indonesia dalam tata kelola data digital regional.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Ilmu Hukum, Universitas Negeri Manado atas dukungan fasilitas dan lingkungan akademik yang kondusif bagi pengembangan penelitian ini. Terima kasih pula kepada para kolega dan reviewer yang telah memberikan masukan konstruktif.

PERNYATAAN KONFLIK KEPENTINGAN

Para penulis menyatakan tidak terdapat konflik kepentingan terkait penelitian, kepengarangan, dan/atau publikasi artikel ini.

DAFTAR PUSTAKA

Astawa, I. G. P., & Sutama, I. K. (2021). Perlindungan data pribadi di era digital: Perspektif hukum Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, 28(2), 345–367. https://doi.org/10.20885/iustum.vol28.iss2.art5

Astawa, I. G. P., & Sutama, I. K. (2021). Perlindungan data pribadi di era digital: Perspektif hukum Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, 28(2), 345–367. https://doi.org/10.20885/iustum.vol28.iss2.art5

Badan Siber dan Sandi Negara. (2022). *Laporan kebocoran data nasional 2022*. BSSN.

Bygrave, L. A. (2020). *Internet governance by contract*. Oxford University Press.

Coglianese, C. (2021). Reflective law and the challenges of regulatory effectiveness. *University of Pennsylvania Law Review*, 169(5), 1311–1360.

Coglianese, C., & Mendelson, E. (2022). *Meta-regulation and self-regulation. In R. Baldwin, M. Cave, & M. Lodge (Eds.), The Oxford handbook of regulation*. Oxford University Press.

European Data Protection Board. (2023). *Decision on the dispute submitted by the Irish supervisory authority regarding Meta Platforms Ireland Limited*. EDPB.

Fajar, M., & Achmad, Y. (2017). *Dualisme penelitian hukum normatif dan empiris (Cetakan IV)*. Pustaka Pelajar.

Fajar, M., & Irwansyah, I. (2025). Tanggung jawab platform e-commerce dalam perlindungan data konsumen: Perspektif UU PDP dan UU Perlindungan Konsumen. *Jurnal Hukum dan Peradilan*, 14(1), 1–22. https://doi.org/10.25216/jhp.14.1.2025

Graham Greenleaf, G. (2021). Global tables of data privacy laws and bills (7th ed.). *Privacy Laws & Business International Report*, 172, 14–26.

Kominfo RI. (2023). *Laporan tahunan perkembangan ekonomi digital Indonesia 2023*. https://www.kominfo.go.id/content/detail/XXXXX/laporan-tahunan/0/highlights

Kominfo RI. (2024). *Laporan tahunan perkembangan ekonomi digital Indonesia 2024*. Kementerian Komunikasi dan Informatika.

Kuner, C. (2022). *Transborder data flows and data privacy law*. Oxford University Press.

Mahkamah Agung Republik Indonesia. (2019). Putusan Nomor 1769 K/Pid.Sus/2019.

Mahkamah Konstitusi Republik Indonesia. (2016). Putusan Nomor 25/PUU-XIV/2016.

Marzuki, P. M. (2019). *Penelitian hukum (Edisi revisi)*. Kencana Prenada Media Group.

Muklish, M., & Wibisana, A. G. (2024). Comparative analysis of Indonesia's Personal Data Protection Law and Singapore's PDPA: Lessons for implementation. *Indonesian Law Review*, 14(3), 233–256. https://doi.org/10.15742/ilrev.v14n3.2024

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Personal Data Protection Act (Singapore), No. 26 of 2012, as amended by the Personal Data Protection (Amendment) Act 2020.

Rahardjo, S. (2014). *Ilmu hukum*. Citra Aditya Bakti.

Ramadhan, R. A., & Prasetyo, B. (2023). Konsep persetujuan dalam Undang-Undang Perlindungan Data Pribadi: Analisis normatif dan perbandingan. *Jurnal Konstitusi*, 20(4), 721–745. https://doi.org/10.31078/jk2044

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 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.

Sinta Dewi, R. (2021). Urgensi regulasi perlindungan data pribadi di Indonesia: Perbandingan dengan GDPR. *Jurnal Hukum IUS QUIA IUSTUM*, 28(1), 1–22. https://doi.org/10.20885/iustum.vol28.iss1.art1

Solove, D. J. (2020). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Solove, D. J., & Schwartz, P. M. (2021). *Information privacy law (6th ed.)*. Wolters Kluwer.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1).

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Nomor 5952).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Voigt, P., & Bussche, A. von dem. (2021). *The EU General Data Protection Regulation (GDPR): A practical guide (2nd ed.)*. Springer.

Wahyudi Djafar, M. (2023). Otoritas pengawas perlindungan data pribadi: Antara independensi dan efektivitas penegakan. *Jurnal Penelitian Hukum De Jure*, 23(2), 189–210. https://doi.org/10.30641/dejure.2023.V23.189-210