

**Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa**

**Gunawan Karnedi<sup>1</sup>, RG Guntur Alam<sup>2</sup>**

<sup>12</sup>Universitas Muhammadiyah Bengkulu

gunawankarnedi24@gmail.com<sup>1</sup>, rggunturalam@umb.ac.id<sup>2</sup>

**ABSTRACT**

*This study aims to evaluate the effectiveness of Indonesia's Personal Data Protection Law No. 27 of 2022 (UU PDP) by comparing it to the European Union's General Data Protection Regulation (GDPR) as an international benchmark. Using a normative and comparative legal approach, this research identifies the strengths and weaknesses of Indonesia's legal framework in safeguarding personal data. The findings reveal that while UU PDP marks a significant step forward in acknowledging data subject rights and introducing legal sanctions, it still lacks comprehensive regulatory mechanisms. Critical areas such as data portability rights, the principle of privacy by design, and clear cross-border data flow regulations remain underdeveloped. Moreover, the absence of an independent supervisory authority limits the enforcement and accountability of the law. Compared to the GDPR, Indonesia's PDP law remains in its early stages of implementation and requires further harmonization with global standards. The study recommends the establishment of an independent data protection authority, issuance of detailed implementing regulations, incorporation of modern data protection principles, and institutional capacity building. With these improvements, Indonesia's data protection regime can become more robust, effective, and aligned with international best practices.*

**Keywords:** personal data protection, PDP Law, GDPR, privacy, comparative regulation

**ABSTRAK**

Penelitian ini bertujuan untuk mengevaluasi efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia dengan membandingkannya terhadap General Data Protection Regulation (GDPR) Uni Eropa sebagai standar internasional. Penelitian menggunakan pendekatan yuridis normatif dan komparatif untuk menilai kekuatan dan kelemahan kerangka hukum Indonesia dalam konteks perlindungan data pribadi. Hasil analisis menunjukkan bahwa meskipun UU PDP menandai kemajuan signifikan melalui pengakuan hak subjek data dan penerapan sanksi terhadap pelanggaran, regulasi ini masih memiliki berbagai keterbatasan struktural dan substantif. Beberapa aspek seperti hak portabilitas data, prinsip *privacy by design*, serta mekanisme aliran data lintas negara belum diatur secara rinci. Selain itu, belum terbentuknya otoritas pengawas independen juga menjadi kelemahan krusial yang dapat menghambat efektivitas implementasi UU PDP. Dibandingkan dengan GDPR, UU PDP masih berada dalam tahap awal perkembangan dan memerlukan harmonisasi dengan standar internasional. Penelitian ini merekomendasikan pembentukan otoritas pengawas independen, penyusunan aturan turunan yang detail, integrasi prinsip perlindungan data modern, dan penguatan kapasitas kelembagaan. Dengan reformasi tersebut, diharapkan perlindungan data pribadi di Indonesia dapat menjadi lebih komprehensif dan setara dengan praktik global.

**Kata Kunci:** perlindungan data pribadi, UU PDP, GDPR, privasi, regulasi komparatif

## **PENDAHULUAN**

Di era digital yang semakin terkoneksi dan bergantung pada teknologi informasi, data pribadi menjadi salah satu aset paling berharga sekaligus paling rentan terhadap berbagai bentuk eksploitasi. Pengumpulan, penyimpanan, dan pemrosesan data pribadi oleh institusi publik maupun swasta menimbulkan kebutuhan mendesak akan kerangka hukum yang kokoh untuk melindungi hak-hak individu atas privasi dan kendali atas informasi pribadi mereka (Maharani & Prakoso, 2024).

Salah satu tantangan utama dalam era digital adalah kebocoran data pribadi, yang kini dipandang sebagai aset bernilai tinggi baik dari sudut pandang individu maupun korporasi karena potensi ekonomisnya. Tingginya nilai tersebut menjadikan data pribadi sebagai sasaran empuk bagi pelaku kejahatan siber. Dampak kebocoran data bukan hanya menyentuh aspek privasi individu, tetapi juga menimbulkan kerugian yang luas, seperti kerusakan reputasi, kerugian finansial, serta tekanan psikologis bagi para korban. Terlebih lagi, insiden semacam ini berpotensi menggerus kepercayaan publik terhadap penyedia layanan digital, yang pada akhirnya dapat menghambat pertumbuhan ekosistem ekonomi digital secara menyeluruh (Ardika, 2025).

Seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi dan platform digital, kebutuhan akan sistem perlindungan data yang lebih ketat menjadi semakin mendesak. Tindak kejahatan seperti pencurian data pribadi yang mencakup peretasan rekening, kecurangan dalam transaksi *e-commerce*, dan akses tidak sah terhadap informasi sensitif, telah menunjukkan eskalasi signifikan. Namun demikian, regulasi pidana yang ada di Indonesia, seperti yang tercantum dalam Pasal 482 dan Pasal 483 KUHP baru, masih belum secara eksplisit mengatur tindak pidana pencurian data secara daring, sehingga perlindungan hukum terhadap konsumen dalam ruang digital dinilai belum memadai (Nuranisa & Lukitasari, 2024).

Di Indonesia, perhatian terhadap isu perlindungan data pribadi mulai menguat seiring dengan meningkatnya kasus kebocoran data yang masif, seperti yang terjadi pada platform *e-commerce* Tokopedia dan layanan publik BPJS Kesehatan, yang mengakibatkan jutaan data pengguna tersebar di forum-forum digital tanpa izin (VOI, 2024). Dalam konteks tersebut, kasus kebocoran data yang dialami oleh Tokopedia pada tahun 2020 menjadi salah satu ilustrasi nyata lemahnya pengamanan data pribadi di Indonesia. Kebocoran yang mengompromikan sekitar 91 juta akun pengguna tersebut menunjukkan bahwa sistem keamanan yang diterapkan perusahaan belum mampu menahan ancaman siber yang terus berkembang (Ardika, 2025). Situasi ini mengangkat persoalan penting mengenai tanggung jawab hukum korporasi, mekanisme ganti rugi bagi konsumen, serta efektivitas regulasi yang telah diberlakukan.

Di sisi lain, upaya global dalam meningkatkan perlindungan data pribadi tercermin dari implementasi General Data Protection Regulation (GDPR) oleh Uni Eropa, yang tidak hanya mengatur tata kelola data pribadi secara ketat tetapi juga menjamin hak-hak individu seperti hak untuk dihapus (*right to be forgotten*) dan hak portabilitas data (*data portability*) (Tolani & Pareek, 2024). Di Indonesia, pengesahan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah progresif yang mencerminkan kesadaran pemerintah akan pentingnya perlindungan data dalam menghadapi tantangan ekosistem digital. Namun, implementasi dan pengawasan terhadap UU ini masih menghadapi sejumlah kendala, termasuk keterbatasan kapasitas lembaga pelaksana, rendahnya literasi digital, serta kesenjangan antara regulasi dengan dinamika teknologi informasi yang terus berkembang pesat (Nuranisa & Lukitasari, 2024). Oleh karena itu, diperlukan evaluasi komprehensif terhadap kesesuaian UU PDP dengan standar internasional, seperti GDPR, guna memperkuat sistem perlindungan data pribadi yang adaptif dan responsif terhadap ancaman digital masa kini.

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mulai berlaku sejak Oktober 2022 dengan masa transisi dua tahun, di mana pengendali dan prosesor data pribadi wajib menyesuaikan aktivitasnya (Ramli, 2023). Meski lembaga pengawas sanksi administratif belum terbentuk, sanksi pidana sudah berlaku efektif. UU PDP memuat sanksi pidana berupa denda dan penjara untuk berbagai pelanggaran, seperti pencurian identitas, pengumpulan, pengungkapan, dan penggunaan data tanpa hak. Kasus pertama yang ditangani adalah Heri Irawan, dihukum lima tahun penjara karena pencurian identitas, serta dua kasus di Tangerang yang melibatkan penjualan kartu SIM dengan NIK curian, masing-masing dihukum 1,5 tahun penjara. Saat ini, sanksi pidana menjadi alat penegakan utama, dan risiko hukum akan meningkat setelah lembaga perlindungan data resmi terbentuk. Oleh karena itu, kepatuhan terhadap UU PDP penting untuk menghindari ancaman sanksi administratif dan pidana (K & K Advocates, 2024).

Berdasarkan latar belakang tersebut, tulisan ini bertujuan untuk menjawab beberapa pertanyaan penelitian yakni (1) sejauh mana efektivitas UU PDP Indonesia bila dibandingkan dengan GDPR Uni Eropa? dan (2) Apa saja kelemahan dan keunggulan yang dapat diidentifikasi dari kerangka regulasi Indonesia dalam melindungi data pribadi warganya? Pertanyaan-pertanyaan ini penting untuk dijawab sebagai dasar dalam melakukan evaluasi mendalam terhadap keberlanjutan kebijakan perlindungan data pribadi nasional dan sebagai upaya untuk mengarahkan Indonesia menuju kesetaraan standar perlindungan data di tingkat global. Tujuan utama penelitian ini adalah untuk mengevaluasi kesesuaian UU PDP Indonesia dengan prinsip-prinsip internasional yang terkandung dalam GDPR serta mengidentifikasi ruang-ruang perbaikan yang dapat dijadikan landasan bagi penguatan regulasi ke depan. Melalui analisis komparatif yang mendalam, studi ini diharapkan dapat memberikan rekomendasi konkret bagi pembuat kebijakan, regulator, dan pemangku kepentingan lainnya di Indonesia untuk memperkuat aspek-aspek substansial maupun kelembagaan dalam perlindungan data pribadi. Selain itu, studi ini diharapkan dapat memberikan kontribusi ilmiah yang signifikan sebagai kajian yang secara sistematis membandingkan UU PDP Indonesia dengan GDPR Uni Eropa, sehingga dapat menjadi referensi akademik maupun praktis dalam diskursus kebijakan data di kawasan Asia Tenggara. Dengan demikian, artikel ini bukan hanya bertujuan untuk mengidentifikasi celah dan potensi dalam kebijakan perlindungan data Indonesia, tetapi juga berupaya membangun jembatan konseptual

dan praktis antara praktik lokal dan standar global, sebagai bentuk respons terhadap tantangan digital masa kini yang bersifat lintas negara dan lintas sektoral.

## **METODE PENELITIAN**

Metode yang diterapkan dalam penelitian ini adalah metode kualitatif. Sebagaimana dijelaskan oleh Moleong (2014), penelitian kualitatif merupakan prosedur yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari individu maupun perilaku yang dapat diamati. Penelitian ini juga menggunakan pendekatan analisis komparatif dan yuridis normatif sebagai landasan utamanya. Pendekatan ini dipilih karena penelitian bertujuan untuk mengeksplorasi, memahami, dan membandingkan secara mendalam aspek normatif dari regulasi perlindungan data pribadi antara Indonesia dan Uni Eropa, khususnya melalui Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia dan General Data Protection Regulation (GDPR) Uni Eropa. Studi ini tidak berfokus pada pengukuran kuantitatif, melainkan pada penafsiran mendalam terhadap teks hukum, dokumen resmi, dan studi kasus yang relevan, yang memungkinkan peneliti untuk mengidentifikasi persamaan, perbedaan, serta implikasi hukum dan praktis dari masing-masing sistem regulasi.

Sumber data dalam penelitian ini terdiri dari data sekunder berupa dokumen-dokumen hukum dan administratif. Data utama yang dianalisis mencakup Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai instrumen hukum Indonesia, serta GDPR sebagai peraturan perlindungan data yang berlaku di seluruh wilayah Uni Eropa.

Metode analisis yang digunakan dalam penelitian ini bersifat deskriptif-komparatif, dengan membandingkan parameter-parameter kunci yang menjadi ciri khas dalam kerangka perlindungan data pribadi masing-masing yurisdiksi (Nazir, 2013). Parameter pertama adalah hak-hak subjek data, termasuk hak untuk mengakses data, hak penghapusan (*right to be forgotten*), serta hak portabilitas data. Selanjutnya, ditinjau pula kewajiban-kewajiban pengontrol data, seperti penunjukan Data Protection Officer (DPO) dan kewajiban notifikasi terhadap pelanggaran data. Parameter ketiga mencakup aspek sanksi dan mekanisme penegakan hukum, baik secara administratif maupun pidana. Terakhir, penelitian ini menelaah pengaturan mengenai aliran data lintas batas (*transborder data flow*), yang menjadi aspek krusial dalam konteks globalisasi digital.

Melalui pendekatan tersebut, penelitian ini berupaya untuk menjawab dua pertanyaan utama: (1) sejauh mana efektivitas UU PDP Indonesia jika dibandingkan dengan GDPR sebagai standar internasional dalam perlindungan data pribadi; dan (2) apa saja keunggulan dan kelemahan yang dapat diidentifikasi dari kerangka hukum Indonesia dalam melindungi data pribadi warganya. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan regulasi perlindungan data yang lebih komprehensif dan aplikatif di Indonesia.

**HASIL DAN PEMBAHASAN**

**Efektivitas UU PDP Indonesia jika Dibandingkan Dengan GDPR sebagai Standar Internasional dalam Perlindungan Data Pribadi**

Efektivitas Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dapat dianalisis melalui pendekatan yuridis normatif dan komparatif terhadap *General Data Protection Regulation* (GDPR) Uni Eropa yang telah diakui secara global sebagai standar emas dalam perlindungan data pribadi. Mengingat UU PDP Indonesia masih tergolong baru dan masih dalam tahap implementasi awal, sedangkan GDPR sudah diberlakukan secara aktif sejak 2018. Terdapat sejumlah aspek yang menunjukkan perbedaan efektivitas antara keduanya. Penelitian ini akan menggunakan data dari *Regulation file GDPR dan UU No. 27 Tahun 2022* serta beberapa penelitian terdahulu yang disusun dalam tabel dan pembahasan sebagai berikut:

**Tabel 1. Komparatif UU PDP Indonesia vs. GDPR Uni Eropa**

No.	Parameter	UU PDP Indonesia	GDPR Uni Eropa
1	<b>Hak Subjek Data</b>	<ul style="list-style-type: none"><li>• Hak untuk mengakses data</li><li>• Hak untuk menghapus data pribadi</li><li>• Tidak mengatur secara eksplisit hak portabilitas data</li></ul>	<ul style="list-style-type: none"><li>• Hak akses, perbaikan, penghapusan (right to be forgotten)</li><li>• Hak portabilitas data (data portability)</li><li>• Hak untuk membatasi dan menolak pemrosesan otomatis</li></ul>
2	<b>Kewajiban Pengontrol Data</b>	<ul style="list-style-type: none"><li>• DPO diwajibkan hanya untuk pengendali tertentu (belum dirinci jelas dalam PP)</li><li>• Wajib memberitahukan pelanggaran data kepada subjek dan otoritas dalam waktu tertentu</li></ul>	<ul style="list-style-type: none"><li>• Wajib menunjuk DPO untuk institusi publik dan pemrosesan berskala besar</li><li>• Wajib melaporkan pelanggaran data dalam 72 jam ke otoritas pengawas dan individu terkait</li></ul>
3	<b>Sanksi dan Penegakan Hukum</b>	<ul style="list-style-type: none"><li>• Sanksi administratif: denda maksimal Rp6 miliar atau 2% pendapatan tahunan</li><li>• Sanksi pidana bagi pelanggaran berat</li><li>• Lembaga pengawas belum terbentuk aktif</li></ul>	<ul style="list-style-type: none"><li>• Sanksi administratif: hingga €20 juta atau 4% dari omzet global, mana yang lebih tinggi</li><li>• Penegakan dilakukan oleh otoritas pengawas independen di tiap negara anggota</li></ul>

4	<b>Mekanisme Transborder Data Flow</b>	<ul style="list-style-type: none"><li>• Belum diatur secara rinci</li><li>• Bergantung pada peraturan pelaksana pemerintah dan kerja sama bilateral</li></ul>	<ul style="list-style-type: none"><li>• Diatur secara ketat</li><li>• Hanya boleh dilakukan ke negara dengan perlindungan setara atau menggunakan instrumen hukum seperti SCC (Standard Contractual Clauses) atau BCR (Binding Corporate Rules)</li></ul>
---	--	---	---

a. Cakupan Hak Subjek Data

GDPR secara eksplisit menetapkan hak-hak subjek data seperti hak akses, hak untuk dilupakan (right to be forgotten), hak pembatasan pemrosesan, hak portabilitas data, dan hak untuk menolak (right to object) (Haristya et al, 2020). UU PDP Indonesia juga mengatur hak serupa, tetapi masih dalam cakupan yang lebih terbatas dan tidak sekomprehensif GDPR. Awwaliyah & Juniarti (2024) menegaskan bahwa GDPR jauh lebih ketat dan memiliki standar perlindungan yang tinggi dibandingkan negara-negara Asia Tenggara terutama dalam menjamin hak atas data pribadi secara konsisten.

b. Kewajiban Pengendali Data dan Penunjukan DPO

Salah satu keunggulan GDPR adalah kewajiban bagi pengendali data untuk menunjuk *Data Protection Officer* (DPO) apabila data yang diproses bersifat masif, sensitif, atau pengawasan secara sistematis dilakukan. Dalam UU PDP Indonesia, kewajiban penunjukan pejabat fungsional yang memiliki fungsi perlindungan data pribadi (setara DPO) juga disebutkan, tetapi masih bersifat opsional dan belum memiliki kejelasan teknis yang mendalam sebagaimana diatur dalam GDPR (Ardika, 2020).

c. Sanksi dan Penegakan Hukum

Efektivitas suatu regulasi juga bergantung pada mekanisme penegakan hukumnya. GDPR memiliki sanksi administratif yang berat hingga 4% dari total pendapatan tahunan global atau €20 juta, tergantung mana yang lebih tinggi. Sebaliknya, UU PDP Indonesia menetapkan sanksi administratif dan pidana, namun belum seketat GDPR dan hingga kini belum ada preseden sanksi yang benar-benar diterapkan secara efektif. Ardika (2020) menyatakan bahwa lemahnya sistem keamanan data dan belum adanya infrastruktur pengawasan yang matang membuat implementasi UU PDP masih penuh tantangan, sebagaimana terlihat dari kasus kebocoran data Tokopedia.

d. Aliran Data Lintas Negara (Cross-Border Data Transfer)

GDPR menetapkan bahwa transfer data lintas batas hanya diperbolehkan ke negara-negara yang memiliki tingkat perlindungan data yang memadai, sementara UU PDP belum memiliki mekanisme yang jelas terkait hal ini. Dalam konteks globalisasi digital, hal ini menjadi titik lemah signifikan karena dapat menghambat arus data internasional dan kolaborasi antarnegara (Hanaya, 2023).

e. Prinsip Transparansi dan Akuntabilitas

GDPR menempatkan transparansi dan akuntabilitas sebagai prinsip utama

perlindungan data pribadi. UU PDP Indonesia sudah mengadopsi prinsip-prinsip serupa dalam Pasal 3 dan Pasal 4, namun dalam praktiknya, pelaksanaannya masih tergantung pada kesiapan institusi pelaksana seperti Kementerian Komunikasi dan Informatika serta BSSN. Seperti diungkapkan Tsamara (2021), Indonesia masih membutuhkan harmonisasi hukum dan kesiapan teknis agar mampu sejajar dengan praktik internasional.

f. Konteks Konstitusional dan Hak Asasi

GDPR berakar pada hak atas privasi yang dilindungi secara konstitusional dan hukum internasional di bawah Pasal 8 *European Convention on Human Rights*. Di Indonesia, hak atas privasi tidak disebutkan secara eksplisit dalam UUD 1945, meskipun Pasal 28F dan 28G memberikan ruang untuk penafsiran tentang hak atas rasa aman dan komunikasi. Haristya et al. (2020) menilai bahwa ketidakhadiran jaminan eksplisit atas privasi ini dapat menyebabkan potensi pelanggaran hak konstitusional warga negara.

Secara normatif, UU PDP Indonesia telah menunjukkan kemajuan signifikan sebagai instrumen hukum nasional yang berupaya menyesuaikan diri dengan standar internasional seperti GDPR, terutama dalam pengakuan terhadap hak subjek data dan upaya menetapkan prinsip perlindungan data. Namun, dari aspek efektivitas, UU PDP masih belum dapat disetarakan dengan GDPR mengingat sejumlah faktor: keterbatasan dalam cakupan hak, belum kuatnya mekanisme penegakan hukum, ketidakjelasan aturan aliran data lintas negara, serta belum adanya perlindungan konstitusional eksplisit terhadap privasi.

Dengan demikian, efektivitas UU PDP Indonesia saat ini masih bersifat potensial dan belum maksimal, terutama dalam konteks implementasi teknis dan budaya perlindungan data yang belum berkembang secara luas. Diperlukan upaya harmonisasi regulasi, penguatan lembaga pengawas, serta edukasi publik untuk meningkatkan efektivitas pelaksanaan UU PDP agar dapat mendekati atau sejajar dengan GDPR.

## **Keunggulan Dan Kelemahan Yang Dapat Diidentifikasi Dari Kerangka Hukum Indonesia Dalam Melindungi Data Pribadi Warganya**

Pembahasan pertanyaan kedua pada penelitian ini disusun berdasarkan hasil analisis deskriptif-komparatif antara Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) GDPR Uni Eropa, serta merujuk pada data sekunder dari laporan resmi dan literatur relevan.

a. Keunggulan Kerangka Hukum Indonesia dalam Melindungi Data Pribadi

a) Eksistensi Payung Hukum Khusus tentang Perlindungan Data Pribadi  
UU PDP merupakan langkah maju yang signifikan dalam pengakuan hak atas data pribadi sebagai bagian dari hak privasi warga negara. Sebelumnya, isu perlindungan data diatur secara sektoral dan tidak terkoordinasi, sehingga keberadaan UU PDP menjadi tonggak penting dalam sistem hukum Indonesia.

b) Pengakuan terhadap Hak Subjek Data

UU PDP memberikan hak-hak dasar bagi subjek data, seperti hak untuk mengakses

dan menghapus data pribadi (Pasal 5 dan 6 UU PDP). Hal ini mencerminkan adopsi prinsip-prinsip internasional dalam GDPR, meskipun belum sepenuhnya lengkap seperti hak atas portabilitas data (Haristya et al, 2020).

c) Sanksi Pidana dan Administratif

UU PDP memuat ancaman sanksi yang cukup kuat, baik secara administratif maupun pidana. Ketentuan ini memberikan efek jera terhadap penyalahgunaan data pribadi, yang tidak ditemukan secara eksplisit dalam banyak regulasi sektoral sebelumnya (UU PDP, Pasal 57-69).

d) Kewajiban Pelaporan Pelanggaran Data

Undang-undang ini mewajibkan pengendali data untuk melaporkan kebocoran data kepada subjek data dan pemerintah, meskipun batas waktunya belum seketat GDPR yang menetapkan 72 jam (Tabel 2. Komparatif PDP-GDPR).

b. Kelemahan Kerangka Hukum Indonesia dalam Melindungi Data Pribadi

a) Belum Terbentuknya Lembaga Pengawas Independen

Salah satu kelemahan paling krusial dari UU PDP adalah belum ditetapkannya otoritas pengawas yang independen dan profesional seperti *Data Protection Authority* dalam GDPR (Pasal 58 UU PDP). Saat ini, kewenangan masih dipegang oleh Kementerian Komunikasi dan Informatika (Kominfo), yang dapat menimbulkan konflik kepentingan karena juga berperan sebagai pembuat kebijakan (Haristya et al, 2020).

b) Minimnya Pengaturan Detail tentang Hak dan Kewajiban

UU PDP belum mengatur secara eksplisit hak atas portabilitas data dan belum mengadopsi prinsip-prinsip *privacy by design*, *privacy by default*, serta penilaian dampak perlindungan data (*Data Protection Impact Assessment/DPIA*) yang menjadi pilar penting GDPR (Greenleaf, 2016).

c) Ketergantungan pada Inisiatif Individu

Tanpa kehadiran lembaga pengawas aktif, beban perlindungan hak lebih besar dibebankan kepada individu. Artinya, subjek data sendiri yang harus mengklaim haknya langsung kepada pengendali data tanpa jaminan mekanisme pengawasan yang independen (Haristya et al, 2020).

d) Kelemahan dalam Pengaturan Aliran Data Lintas Batas

Pengaturan mengenai *transborder data flow* dalam UU PDP masih terbatas dan belum mencantumkan standar perlindungan data memadai sebagai syarat transfer data ke luar negeri, yang merupakan syarat utama dalam GDPR (GDPR, Pasal 44-50).

e) Kurangnya Harmonisasi dengan Standar Regional

Indonesia tertinggal dari negara-negara tetangga di ASEAN seperti Singapura, Malaysia, dan Thailand yang telah membentuk kerangka hukum data pribadi dan otoritas pengawas yang berfungsi secara aktif (Gribakov, 2019).

Meskipun GDPR sering dipandang sebagai standar emas dalam perlindungan data pribadi di tingkat global, sejumlah kritik penting telah disampaikan oleh akademisi dan praktisi. Salah satunya terkait kesenjangan antara prinsip yang diatur dalam GDPR dengan implementasi di lapangan. Beberapa studi menyebutkan bahwa penegakan hukum GDPR terhadap pelanggaran, khususnya yang dilakukan oleh perusahaan teknologi raksasa, cenderung lamban dan tidak merata antar negara anggota Uni Eropa, sehingga mengurangi daya efektifnya sebagai regulasi

perlindungan data yang kuat (Cristofidou et al., 2021). Selain itu, hak portabilitas data dalam GDPR juga dianggap belum sepenuhnya memberikan kendali kepada individu atas data mereka, karena hanya mencakup data yang diberikan secara langsung, sementara data yang diperoleh melalui pelacakan aktivitas pengguna justru dikecualikan. Tidak hanya itu, beberapa pihak juga mempertanyakan kelayakan GDPR sebagai model global, mengingat perbedaan pendekatan antara Uni Eropa, Amerika Serikat, dan negara-negara Asia terhadap isu privasi dan keamanan data (Bradford, 2020). Kritik-kritik ini menunjukkan bahwa meskipun GDPR menjadi rujukan utama, regulasi tersebut masih memiliki keterbatasan yang patut dicermati. Lebih lanjut, berbagai studi menganjurkan pentingnya pendekatan multidisipliner dalam merancang dan mengimplementasikan regulasi perlindungan data pribadi (Surahman & Annisarizki, 2024). Perlindungan data bukan hanya isu hukum, tetapi juga berkaitan erat dengan perkembangan teknologi, etika digital, dan dimensi sosial budaya masyarakat. Dwivedi (2022) dalam penelitiannya menegaskan bahwa kolaborasi antara ahli hukum, insinyur teknologi, dan akademisi dari berbagai disiplin sangat diperlukan untuk merumuskan kebijakan data pribadi yang efektif dan aplikatif. Pendekatan tunggal yang hanya menekankan aspek hukum seringkali gagal mengantisipasi tantangan teknologi digital modern seperti *cloud computing*, *big data analytics*, dan *AI-driven decision-making* yang terus berkembang. Dalam konteks Indonesia, pembelajaran dari tantangan implementasi GDPR dan pentingnya pendekatan multidisipliner ini menjadi relevan untuk memastikan bahwa UU PDP tidak hanya kuat secara normatif, tetapi juga responsif terhadap kebutuhan teknis, sosial, dan etis di era digital saat ini.

## **KESIMPULAN**

Berdasarkan hasil analisis yuridis normatif dan komparatif antara Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Indonesia dengan General Data Protection Regulation (GDPR) Uni Eropa sebagai standar internasional, dapat disimpulkan bahwa meskipun UU PDP Indonesia merupakan kemajuan penting dalam sistem hukum nasional, efektivitasnya masih bersifat potensial dan belum sepenuhnya optimal. UU PDP telah mengakomodasi sejumlah prinsip dasar perlindungan data pribadi, seperti pengakuan terhadap hak subjek data, sanksi pidana dan administratif, serta kewajiban pelaporan pelanggaran data. Hal ini menunjukkan adanya upaya harmonisasi terhadap praktik perlindungan data global.

Namun demikian, dibandingkan dengan GDPR, UU PDP masih memiliki beberapa kelemahan mendasar yang berdampak pada efektivitasnya, antara lain: cakupan hak subjek data yang belum komprehensif, ketidaktegasan dalam kewajiban pengendali data, lemahnya mekanisme penegakan hukum akibat belum terbentuknya lembaga pengawas independen, serta belum memadainya pengaturan aliran data lintas negara. Selain itu, belum diaturnya prinsip-prinsip modern seperti *privacy by design*, *privacy by default*, dan *Data Protection Impact Assessment (DPIA)* turut memperlihatkan jarak antara kerangka hukum Indonesia dengan GDPR.

Di sisi lain, kehadiran GDPR sebagai standar global juga bukan tanpa kritik. Sejumlah studi menunjukkan adanya tantangan implementasi di lapangan,

kesenjangan penegakan hukum antarnegara anggota, hingga keterbatasan cakupan hak portabilitas data. Hal ini menandakan bahwa efektivitas sebuah regulasi perlindungan data pribadi tidak hanya ditentukan oleh ketentuan normatif, melainkan juga oleh kesiapan infrastruktur hukum, budaya kepatuhan, kapasitas institusi pengawas, dan partisipasi publik.

Dengan demikian, untuk meningkatkan efektivitas UU PDP Indonesia agar dapat sejajar dengan standar internasional, diperlukan langkah strategis berupa penyusunan regulasi turunan yang komprehensif, percepatan pembentukan otoritas pengawas independen, penguatan mekanisme pengawasan dan penegakan hukum, serta peningkatan literasi masyarakat terkait hak-hak atas data pribadi. Selain itu, harmonisasi dengan standar regional dan adaptasi terhadap dinamika perkembangan teknologi informasi juga menjadi keharusan agar Indonesia mampu membangun sistem perlindungan data pribadi yang kuat, adaptif, dan relevan di tingkat global. Berdasarkan temuan dan perbandingan tersebut, beberapa saran yang dapat diajukan untuk meningkatkan efektivitas perlindungan data pribadi di Indonesia adalah sebagai berikut:

1. Pembentukan Otoritas Pengawas Independen
  - a. Kebijakan: Segera membentuk lembaga pengawas perlindungan data pribadi yang independen, tidak berada di bawah kementerian mana pun, sebagaimana konsep *Data Protection Authority* dalam GDPR.
  - b. Alasan teknis: Independensi diperlukan agar pengawasan dapat berjalan objektif dan bebas dari konflik kepentingan. Lembaga ini harus memiliki kewenangan penyidikan administratif, audit, serta wewenang menjatuhkan sanksi.
2. Penyusunan dan Penerbitan Peraturan Pelaksana (PP) dan SOP Teknis
  - a. Kebijakan: Menyusun peraturan pelaksana secara detail tentang:
    - a) Penunjukan dan peran fungsional Pejabat Perlindungan Data (*Data Protection Officer*),
    - b) Prosedur pelaporan pelanggaran data termasuk tenggat waktu maksimal (misal, 72 jam),
    - c) Standar perlindungan dalam transfer data lintas negara.
  - b. Alasan teknis: Peraturan ini penting agar pelaku usaha dan instansi pemerintah memiliki pedoman operasional yang jelas dan terukur.
3. Integrasi Prinsip “Privacy by Design” dan “Privacy by Default” dalam Sistem Digital
  - a. Kebijakan: Mewajibkan seluruh sistem teknologi informasi yang mengelola data pribadi untuk menerapkan prinsip *privacy by design* (perlindungan sejak awal perancangan sistem) dan *privacy by default* (pengaturan default harus menjamin privasi).
  - b. Langkah teknis: Pengembangan standar sistem informasi nasional berbasis *compliance* terhadap prinsip-prinsip tersebut, misalnya melalui sertifikasi ISO/IEC 27701.
4. Penguatan Pengaturan Transborder Data Flow
  - a. Kebijakan: Merumuskan mekanisme legal transfer data lintas negara dengan menetapkan daftar negara yang memiliki perlindungan setara (*adequacy decision*),

atau melalui skema seperti *Standard Contractual Clauses* (SCC) atau *Binding Corporate Rules* (BCR).

b. Alasan teknis: Untuk mendukung transformasi digital dan e-commerce lintas negara, sambil menjaga keamanan dan kedaulatan data nasional.

5. Implementasi Mekanisme DPIA (Data Protection Impact Assessment)

a. Kebijakan: Mewajibkan seluruh organisasi yang mengelola data berskala besar atau sensitif untuk melakukan penilaian dampak perlindungan data (DPIA) secara berkala.

b. Langkah teknis: Kominfo dan BSSN dapat menyusun pedoman DPIA dan mewajibkan laporan DPIA diserahkan ke otoritas pengawas secara berkala.

6. Peningkatan Edukasi dan Literasi Data bagi Publik dan Pelaku Usaha

a. Kebijakan: Meluncurkan program nasional literasi data pribadi yang melibatkan media, sektor pendidikan, dan komunitas digital.

b. Langkah teknis: Pemerintah bisa bekerja sama dengan penyedia platform digital untuk menyisipkan *privacy awareness module* pada onboarding pengguna serta mendorong kurikulum perlindungan data di jenjang pendidikan tinggi dan vokasi.

7. Harmonisasi UU PDP dengan Peraturan Regional dan Internasional

a. Kebijakan: Menjalin kerja sama bilateral dan multilateral dalam perlindungan data, terutama dengan negara-negara ASEAN untuk mendorong harmonisasi standar.

b. Alasan teknis: Harmonisasi ini akan memudahkan transfer data legal antarwilayah dan meningkatkan daya saing sektor digital Indonesia secara regional.

8. Penetapan Target dan Indikator Evaluasi Implementasi UU PDP

a. Kebijakan: Menyusun roadmap nasional implementasi UU PDP dengan target waktu dan indikator yang dapat diukur, seperti jumlah organisasi yang menunjuk DPO, jumlah DPIA, serta tingkat pelaporan kebocoran data.

b. Langkah teknis: Menugaskan lembaga pengawas untuk mengeluarkan laporan tahunan perlindungan data pribadi secara transparan kepada publik.

Dengan rekomendasi-rekomendasi tersebut, diharapkan UU PDP tidak hanya menjadi simbol komitmen terhadap perlindungan data pribadi, tetapi juga mampu berfungsi secara efektif dalam praktik, serta memberikan perlindungan yang setara dengan standar global yang diwakili oleh GDPR.

**DAFTAR PUSTAKA**

- Ardika, I. W. C. (2025). Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce. *Indonesian Journal of Law and Justice*, 2(3), 1–11. <https://doi.org/10.47134/ijl.v2i3.3601>
- Awwaliyah, R. P., & Juniarti, S. (2024). *Perbandingan General Data Protection Regulation (GDPR) dengan regulasi perlindungan data di negara-negara Asia Tenggara*. *CAUSA: Jurnal Hukum dan Kewarganegaraan*, 4(4). <https://doi.org/10.3783/causa.v2i9.2461>
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Christofidou, M., Lea, N., & Coorevits, P. (2021). A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. *Yearbook of medical informatics*, 30(1), 226–232. <https://doi.org/10.1055/s-0041-1726512>
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y. G., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K.-B., Papagiannidis, S., Pappas, I. O., Polyviou, A., Park, S.-M., Pandey, N., Queiroz, M. M., Raman, R., Rauschnabel, P. A., Shirish, A., Sigala, M., Spanaki, K., Tan, G. W.-H., Tiwari, M. K., Viglia, G., & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>
- European Union. (2016). *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)*. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Greenleaf, G. (2016, January 30). International data privacy agreements after the GDPR and Schrems. *Privacy Laws & Business International Report*, 139, 12–15.
- Gribakov, A. (2019). *Cross-border privacy rules in Asia: An overview*. Lawfare. <https://www.lawfaremedia.org/article/cross-border-privacy-rules-asia-overview>
- Hanaya, E. (2023). *Perlindungan data pribadi di era digital dalam perspektif perbandingan hukum*. *Jurnal Bevinding*, 1(9), 11–20.
- Haristya, S., Laksmi, S., Astuti, A. N. T., & Dewi, I. F. (2020). *Studi pendahuluan: Perbandingan rancangan undang-undang perlindungan data pribadi dengan Konvensi Eropa 108+ dan GDPR*. Jakarta: Tifa Foundation.
- K & K Advocates. (2024). *Kasus-kasus awal dari implementasi sanksi pidana dalam UU PDP*. Diakses melalui <https://kk-advocates.com/news/read/kasus-awal->

implementasi-sanksi-pidana-dalam-uu-pdp

- Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal USM Law Review*, 7(1), 333-347.
- Nazir, M. (2013). *Metode Penelitian*. Bogor: Ghalia Indonesia
- Nuranisa, A., & Lukitasari, D. (2024). Tindak pidana pencurian data dan privasi pengguna dalam transaksi e-commerce (Studi kasus pada aplikasi Tokopedia). *Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia*, 1(2), 115-126. <https://doi.org/10.62383/amandemen.v1i2.145>
- Pemerintah Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Ramli, A. M. (2023). *Pemrosesan data pribadi menurut UU PDP dan status eksisting*. Kompas.com. Diakses melalui <https://nasional.kompas.com/read/2023/03/23/11333391/pemrosesan-data-pribadi-menurut-uu-pdp-dan-status-eksisting?page=all>
- Surahman, S., & Annisarizki, A. (2024). *Memahami kajian media dan budaya: Pendekatan multidisipliner*. Kencana Media Prenada.
- Tsamara, N. (2021). Perbandingan aturan perlindungan privasi atas data pribadi antara Indonesia dengan beberapa negara. *Jurnal Suara Hukum*, 3(1), 1-15. <https://doi.org/10.2656/534X.v3i1>
- Tolani, C., & Pareek, J. (2024). Introduction to data protection frameworks: A review. *International Journal of Advanced Research in Science, Communication and Technology*, 2024(4), 251-255. <https://doi.org/10.48175/ijarsct-18732>
- VOI, (2024). *Kebobolan BPJS dan Bagaimana Data Pribadi Kita Diperjualbelikan Secara Ilegal*. Diakses melalui <https://voi.id/bernas/53261/kebobolan-bpjs-dan-bagaimana-data-pribadi-kita-diperjualbelikan-secara-ilegal>