



Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks

Perlindungan Data Pribadi di ASEAN: Perbandingan Kritis antara Kerangka Hukum Indonesia dan Malaysia

Putu Aryan Darma Sukerta^{a,1} Andri Sutrisno^{b,2}

^aIBLAM School of Law, Jakarta, Indonesia

^bIBLAM School of Law, Jakarta, Indonesia

¹ Putu.Aryan@gmail.com * ² andrisutrisno@iblam.ac.id

Corresponding author*

ARTICLE INFO

Article history

Received: 23 August 2024

Revised: 01 September 2024

Accepted: 14 September 2024

Keywords

Personal Data Protection;
Comparative Legal Analysis;
Regulatory Enforcement;
Data Subject Rights

ABSTRACT

The development of digital technology presents significant challenges in personal data protection amid globalization and cross-border data exchange. This study compares Indonesia's Personal Data Protection Act (UU PDP) and Malaysia's Personal Data Protection Act (PDPA) 2010 from a normative and doctrinal legal perspective. Using a comparative legal approach through literature review, this research analyzes data subject rights, application mechanisms, supervisory structures, and enforcement and sanctioning mechanisms in both jurisdictions. The findings indicate that Indonesia's UU PDP is more comprehensive as it covers both the public and private sectors, regulates formal procedures for data access, correction, deletion, and consent withdrawal, and is supported by strict administrative and criminal sanctions. In contrast, Malaysia's PDPA applies only to commercial transactions, relying on lighter administrative sanctions, potentially leaving gaps in public sector data protection. Both countries also face challenges regarding the independence of supervisory bodies. This study highlights the need for institutional reforms and regulatory adjustments in line with international standards to enhance transparency, accountability, and legal certainty in personal data protection across ASEAN.

This is an open access article under the [CC-BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/) license.



1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah mengubah berbagai aspek kehidupan manusia secara signifikan.¹ Di tengah kemajuan ini, muncul tantangan baru yang serius, khususnya dalam hal perlindungan data pribadi.² Peningkatan insiden peretasan dan penyalahgunaan data, seperti yang dilaporkan oleh perusahaan keamanan siber Surfshak, menunjukkan tren peningkatan eksponensial dalam pelanggaran data. Misalnya, pada 15 April 2024, negara-negara seperti Amerika Serikat, Rusia, dan Cina mencatatkan tingkat kebocoran data tertinggi,³ sementara Indonesia menempati posisi di antara 10 besar negara dengan tingkat kebocoran data terbanyak di dunia.⁴

Fenomena kebocoran data di Indonesia tidak lepas dari sejumlah insiden signifikan yang terjadi antara Januari 2020 hingga Juli 2024. Insiden pada platform e-commerce Tokopedia pada tahun 2020, di mana sebanyak 91 juta akun dilaporkan diretas⁵, serta serangan terhadap Pusat Data Nasional (PDN) pada Juli 2024 yang mengganggu layanan sejumlah instansi pemerintah,⁶ mengindikasikan adanya kerentanan serius dalam sistem perlindungan data nasional. Kasus-kasus tersebut juga mengungkap bahwa pembelajaran

¹ Mustafa et al., *Kampus Merdeka*, CV Bintang Semesta Media (Yogyakarta: Bintang Semesta Media, 2023).

² Ferinda K Fachri, "Deputi BSSN: Penyebab Kebocoran Data Pribadi Biasanya Kepatuhan Hukum yang Kurang," *Hukum Online*, 2024, <https://www.hukumonline.com/berita/a/deputi-bssn--penyebab-kebocoran-data-pribadi-biasanya-kepatuhan-hukum-yang-kurang-lt6644ead0802f8/?page=2>.

³ Andika Dwi, "10 Negara dengan Kasus Kebocoran Data Terbanyak, Mirip PDN Indonesia," *Tempo.co*, 2024.

⁴ Adi Ahdiat, "Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar," <https://databoks.katadata.co.id>, 2024, <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>.

⁵ Roy Franedy, "91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M," *CNBC Indonesia*, 2020, 1–5; Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data)," in *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 2020, 43–60, <http://jurnal.unissula.ac.id/index.php/PH/article/view/1476>.

⁶ Viriya Singgih, "Petinggi Kominformundur 'sebagai tanggung jawab moral' setelah Pusat Data Nasional diretas," *BBC News Indonesia*, 2024, 1–21, <https://www.bbc.com/indonesia/articles/c8vdmymynzo>.

dari insiden sebelumnya tampaknya belum optimal dalam upaya memperkuat keamanan data.⁷

Di sisi lain, meskipun Malaysia telah mengimplementasikan Personal Data Protection Act (PDPA) 2010, pelanggaran data masih kerap terjadi. Laporan dari Cyberthreat.id mencatat adanya 11 insiden kebocoran data pada periode 2021–2022.⁸ Hal ini menimbulkan pertanyaan mengenai efektivitas implementasi regulasi perlindungan data di kedua negara, terutama dalam konteks pelaksanaan dan pengawasan.

Pelanggaran data pribadi yang terjadi di Indonesia dan Malaysia menimbulkan kekhawatiran mendalam tentang sejauh mana kerangka hukum yang ada dapat memberikan perlindungan yang memadai. Meskipun masing-masing negara telah mengesahkan peraturan untuk melindungi data pribadi,⁹ terdapat tantangan nyata dalam implementasi dan pengawasan, terutama terkait dengan inkonsistensi dalam penegakan hukum. Di Indonesia, misalnya, tantangan tambahan muncul akibat isu independensi lembaga pengawas sebagaimana diamanatkan dalam Pasal 58–60 Undang-Undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP), di mana lembaga pengawas ditempatkan di bawah Presiden dan bertanggung jawab langsung kepadanya, sehingga berpotensi menghambat efektivitas penegakan hukum.¹⁰

Penelitian terkait perlindungan data pribadi di ASEAN telah berkembang, dengan sejumlah studi komparatif yang menyoroiti perbedaan regulasi antarnegara. Studi sebelumnya seperti Muhammad Saiful Rizal (2019) menekankan bahwa penting bagi Indonesia untuk menghadirkan regulasi yang mengatur perlindungan data pribadi sebagaimana regulasi yang ada di Malaysia.¹¹ Penelitian yang dilakukan oleh Fahreza Dabiswara dan Faiz Rahman (2018) dengan tema Perlindungan Data Pribadi : Studi

⁷ Ghita Intan, “Pusat Data Nasional Diretas, Pakar: Pemerintah Tak Pernah Belajar dari Kesalahan,” *VOA Indonesia.com*, 2024, 1–5, <https://www.voaindonesia.com/a/pusat-data-nasional-diretas-pakar-pemerintah-tak-pernah-belajar-dari-kesalahan/7682298.html>.

⁸ Niken Razaq, “11 Kasus Kebocoran Data di Malaysia Dua Tahun Terakhir,” *cyberthreat.id*, 2023, <https://cyberthreat.id/read/15129/11-Kasus-Kebocoran-Data-di-Malaysia-Dua-Tahun-Terakhir>.

⁹ Indonesia memiliki Undang-Undang No. 27 Tahun 2020 tentang Perlindungan Data Pribadi dan Malaysia memiliki *The Malaysia Personal Data Protection Act 2010* (Undang-Undang Perlindungan Data Pribadi Malaysia 2010)

¹⁰ Mochamad Januar Rizki, “Menyorot Independensi Lembaga Pengawas Data Pribadi,” *Hukum Online.com*, 2023, <https://www.hukumonline.com/berita/a/menyorot-independensi-lembaga-pengawas-data-pribadi-lt6461f9e088aeb>.

¹¹ Muhammad Saiful Rizal, “Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia,” *Jurnal Cakrawala Hukum* 10, no. 2 (2019): 218–27, <https://doi.org/10.26905/idjch.v10i2.3349>.

komparasi Terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia. Dalam temuannya, mereka menekankan bahwa Malaysia memiliki lembaga khusus yang memiliki kewenangan untuk menangani perlindungan data pribadi. Dan olehnya itu mereka berkesimpulan bahwa urgen bagi Indonesia untuk menghadirkan lembaga yang memiliki kewenangan khusus untuk menangani perlindungan data pribadi.¹² Namun, masih sedikit penelitian yang secara kritis menganalisis dampak perbedaan institusional ini terhadap efektivitas perlindungan data di tingkat praktis. Penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan menyajikan analisis komparatif antara UU PDP Indonesia dan PDPA Malaysia, khususnya dalam konteks independensi pengawasan.

Nilai kebaruan dari penelitian ini terletak pada pendekatan komparatif yang digunakan untuk menganalisis dua sistem hukum yang berbeda namun berada dalam kerangka regional yang sama. Penelitian ini tidak hanya memberikan analisis hukum normatif tetapi juga mempertimbangkan implikasi praktis dari perbedaan ini terhadap pelaksanaan perlindungan data pribadi di lapangan. Dengan demikian, penelitian ini memberikan kontribusi penting dalam perumusan kebijakan yang lebih efektif untuk perlindungan data pribadi di Indonesia dan Malaysia.

Lebih lanjut, penelitian ini menyoroti pentingnya reformasi kelembagaan dalam memastikan bahwa perlindungan data pribadi di ASEAN dapat berjalan efektif dan sesuai dengan standar internasional. Hasil penelitian ini diharapkan dapat memberikan masukan yang berharga bagi pembuat kebijakan di Indonesia dan Malaysia dalam mengatasi masalah independensi pengawasan dan meningkatkan efektivitas pelaksanaan hukum perlindungan data pribadi.

Penelitian ini tidak hanya penting untuk mengisi gap dalam literatur terkait perlindungan data pribadi di ASEAN tetapi juga memiliki implikasi praktis yang signifikan. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pembuat kebijakan di Indonesia dan Malaysia untuk memperbaiki regulasi yang ada, khususnya dalam hal independensi lembaga pengawas. Selain itu, penelitian ini juga berkontribusi pada pengembangan teori hukum mengenai perlindungan data pribadi di wilayah yang memiliki keragaman institusional seperti ASEAN.

2. Materi Hukum dan Metode Penelitian

Penelitian ini merupakan jenis penelitian hukum normatif atau doktrinal, yaitu penelitian yang berfokus pada kajian norma-norma hukum yang terkandung dalam peraturan perundang-undangan. Pendekatan yang digunakan dalam penelitian ini adalah

¹² Fahreza Daniswara dan Faiz Rahman, "Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia," *Center For Digital Society* 31 (2018): 24.

pendekatan perbandingan hukum (*comparative study*), dengan membandingkan ketentuan hukum positif terkait perlindungan data pribadi antara Indonesia dan Malaysia, terutama setelah disahkannya Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Data penelitian diperoleh melalui studi kepustakaan yang mencakup literatur hukum, peraturan perundang-undangan, jurnal, dan dokumen resmi lainnya, dan selanjutnya dianalisis menggunakan teknik analisis deskriptif kualitatif.

3. Pembahasan

3.1 Independensi Otoritas Pengawas dalam Perlindungan Data Pribadi: Studi Komparatif antara Indonesia dan Malaysia

Perkembangan digital yang pesat telah menuntut perlunya regulasi yang efektif dalam melindungi data pribadi. Di Indonesia, misalnya, hingga saat ini otoritas pengawas perlindungan data pribadi secara kelembagaan belum terbentuk karena masih menunggu penetapan dari Presiden. Meskipun demikian, secara normatif, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengamanatkan pembentukan lembaga tersebut. Pasal 58 ayat (2) dan (3) menetapkan bahwa penyelenggaraan perlindungan data pribadi harus dilakukan oleh suatu lembaga yang ditetapkan oleh Presiden dan bertanggung jawab langsung kepadanya¹³ Dengan demikian, meskipun lembaga ini belum beroperasi secara aktual, perannya telah ditetapkan sebagai bagian integral dari sistem pengelolaan data pribadi di Indonesia.

Selanjutnya, UU PDP memberikan dasar hukum yang kuat bagi lembaga pengawas melalui rincian tugas dan wewenang yang tertuang dalam Pasal 59. Pasal tersebut menguraikan empat fungsi utama Pertama, perumusan dan penetapan kebijakan yang menjadi pedoman bagi berbagai pihak, termasuk Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi. Kedua, pengawasan terhadap kepatuhan guna memastikan bahwa semua entitas yang terlibat dalam pengolahan data pribadi menjalankan kewajibannya sesuai dengan regulasi yang berlaku. Ketiga, penegakan hukum administratif, termasuk kewenangan menjatuhkan sanksi atau memberikan peringatan atas pelanggaran terhadap UU PDP. Keempat, fasilitasi penyelesaian sengketa di luar pengadilan sebagai mekanisme alternatif dalam menangani perselisihan terkait perlindungan data pribadi.

Selain itu, Pasal 60 UU PDP menegaskan peran strategis lembaga pengawas dengan memberikan kewenangan tambahan, seperti merumuskan kebijakan regulasi,

¹³ Gunawan Widjaja dan Fransiska Milenia Cesarianti, “Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi,” *SINERGI: Jurnal Riset Ilmiah* 1, no. 4 (2024): 234–42, <https://doi.org/10.62335/8qf44b59>.

melakukan investigasi atas dugaan pelanggaran, dan menjalin kerja sama internasional. Secara spesifik, lembaga ini juga bertugas mengawasi kepatuhan pengendali data, menjatuhkan sanksi administratif, dan mendukung aparat penegak hukum dalam menangani kasus pidana yang berkaitan dengan data pribadi. Lebih lanjut, lembaga ini memiliki kewenangan dalam melakukan evaluasi terhadap transfer data ke luar negeri, memberikan rekomendasi tindak lanjut atas hasil pengawasan, serta mempublikasikan temuan kepatuhan sesuai ketentuan yang berlaku.

Di sisi lain, pendekatan Indonesia dalam mengatur perlindungan data pribadi dibandingkan dengan Malaysia menunjukkan perbedaan yang cukup mendasar. Malaysia telah lebih dahulu mengatur perlindungan data pribadi melalui *Personal Data Protection Act* (PDPA) 2010 (Act 709), yang membentuk *Personal Data Protection Commissioner* (PDPC) sebagai otoritas pengawas utama. PDPC berada di bawah Kementerian Komunikasi dan Digital Malaysia dan bertanggung jawab atas pengawasan kepatuhan, penerapan sanksi administratif, serta penyelesaian sengketa terkait data pribadi.¹⁴ Selain itu, Malaysia juga memiliki *Personal Data Protection Department* (JPDP) yang didirikan pada 16 Mei 2011 sebagai lembaga pelaksana yang mengawasi kepatuhan sektor publik dan swasta dalam pemrosesan data pribadi, khususnya dalam transaksi komersial.¹⁵

Jika dibandingkan dengan model yang dirancang dalam UU PDP Indonesia, PDPA Malaysia memiliki cakupan yang lebih terbatas, karena hanya berlaku dalam konteks transaksi komersial dan tidak mengikat sektor publik.¹⁶ Pasal 2(1) PDPA 2010 secara eksplisit membatasi lingkup regulasi pada pemrosesan data pribadi dalam aktivitas bisnis, sehingga otoritas pengawas Malaysia tidak memiliki yurisdiksi terhadap pengelolaan data yang dilakukan oleh lembaga pemerintah. Dengan demikian, JPDP lebih berperan sebagai pengawas kepatuhan sektor swasta, dibandingkan sebagai regulator perlindungan data pribadi secara menyeluruh. Fungsi utama JPDP meliputi pengawasan pemrosesan data dalam transaksi komersial, perlindungan konsumen dari penyalahgunaan data, serta registrasi pengguna data pribadi, di mana semua entitas non-pemerintah yang memproses data pribadi diwajibkan untuk terdaftar secara resmi guna menjamin kepatuhan terhadap regulasi yang berlaku.

¹⁴ Komisioner Perlindungan Data Pribadi (PPDP) adalah lembaga di bawah Kementerian Digital Malaysia yang dibentuk pada 15 November 2013 setelah disahkannya Undang-Undang Perlindungan Data Pribadi 2010 (APDP), yaitu Undang-Undang No. 709. PPDP bertanggung jawab atas pengaturan pemrosesan data pribadi dalam transaksi komersial serta penegakan kebijakan perlindungan data pribadi, sumber <https://www.pdp.gov.my/ppdpv1/en/ppdp-eng/>

¹⁵ <https://www.pdp.gov.my/ppdpv1/en/personal-data-protection-department/>

¹⁶ Ali Alibeigi dan Abu Bakar Munir, "Malaysian personal data protection act, a mysterious application," *University of Bologna Law Review* 5, no. 2 (2020): 362–74, <https://doi.org/10.6092/ISSN.2531-6133/12441>.

Dari perspektif independensi kelembagaan, baik Indonesia maupun Malaysia menghadapi tantangan serupa, karena otoritas pengawas perlindungan data pribadi mereka masih berada dalam struktur pemerintahan. Di Indonesia, lembaga yang akan dibentuk berada langsung di bawah Presiden, yang berpotensi menimbulkan keterbatasan dalam independensi operasionalnya.¹⁷ Sementara itu, di Malaysia, PDPC dan JPDP beroperasi di bawah Kementerian Komunikasi dan Digital, sehingga tetap memiliki keterikatan struktural dengan pemerintah. Model ini berbeda dengan beberapa negara lain yang menerapkan sistem pengawasan data pribadi yang lebih independen.¹⁸

Dalam konteks standar global, Uni Eropa telah menetapkan prinsip independensi bagi otoritas pengawas perlindungan data pribadi melalui General Data Protection Regulation (GDPR). Pasal 52 GDPR secara eksplisit mengatur bahwa otoritas perlindungan data harus bersifat independen dan bebas dari campur tangan pemerintah atau entitas lain dalam menjalankan tugasnya.¹⁹ Negara-negara seperti Jerman dan Prancis telah menerapkan prinsip ini dengan memberikan kewenangan penuh kepada otoritas pengawasnya agar dapat bertindak secara mandiri dalam menegakkan kebijakan perlindungan data pribadi. Dengan model ini, pengawasan terhadap pengelolaan data pribadi tidak hanya bersifat normatif tetapi juga memiliki efektivitas hukum yang lebih kuat, memastikan kepatuhan yang lebih ketat dari sektor publik maupun swasta.

Jika dibandingkan dengan standar yang ditetapkan dalam GDPR, baik Indonesia maupun Malaysia belum sepenuhnya memenuhi prinsip independensi dalam pengawasan perlindungan data pribadi. Struktur kelembagaan yang masih berada dalam pengaruh eksekutif dapat menimbulkan potensi konflik kepentingan, terutama jika kebijakan yang dibuat tidak sepenuhnya bebas dari intervensi politik atau kepentingan bisnis. Meskipun Malaysia telah lebih dahulu memiliki regulasi dan otoritas pengawas yang beroperasi, cakupan yurisdiksinya yang terbatas pada transaksi komersial menjadi tantangan tersendiri dalam menjamin perlindungan data pribadi secara menyeluruh.

Dengan mempertimbangkan perbedaan ini, Indonesia memiliki peluang untuk membangun otoritas pengawas yang lebih independen dibandingkan Malaysia, terutama jika dalam implementasinya nanti lembaga ini dapat beroperasi secara otonom dan tidak sekadar menjadi bagian dari struktur eksekutif. Namun, dengan kedudukannya di bawah

¹⁷ Juan Matheus dan Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *Justisi* 10, no. 1 (2023): 20–35, <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.

¹⁸ Wahyudi Djafar dan M. Jodi Santoso, *PERLINDUNGAN DATA PRIBADI: Pentingnya Otoritas Pengawasan Independen, Lembaga Studi dan Advokasi Masyarakat (ELSAM)*, 2019.

¹⁹ Denico Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru," *Negara Hukum* 12, no. 2 (2021): 227.

Presiden, masih terdapat potensi kendala dalam menjamin independensi penuh. Untuk mencapai efektivitas perlindungan data pribadi yang optimal, Indonesia perlu menyeimbangkan antara kepentingan regulasi, independensi lembaga, dan kepatuhan terhadap standar internasional, termasuk dengan mengadopsi prinsip-prinsip dalam GDPR yang menekankan transparansi, akuntabilitas, dan otonomi penuh bagi otoritas pengawas.

3.2. Hak Subjek Data dan Implementasi Kebijakan Perlindungan Data di Indonesia dan Malaysia

Perlindungan data pribadi merupakan aspek fundamental dalam regulasi digital yang bertujuan untuk memastikan hak subjek data tetap terjaga dalam setiap proses pengolahan data.²⁰ Indonesia dan Malaysia, sebagai dua negara di Asia Tenggara, telah mengadopsi regulasi perlindungan data dengan pendekatan yang berbeda. Di Indonesia, regulasi ini tertuang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sedangkan Malaysia telah lebih dahulu menerapkan Personal Data Protection Act (PDPA) 2010 (Act 709). Perbandingan antara kedua regulasi ini menjadi relevan dalam menilai sejauh mana perlindungan hak subjek data telah diterapkan, serta bagaimana kebijakan tersebut diimplementasikan dalam sistem hukum masing-masing negara.

Dalam konteks hak subjek data, baik UU PDP Indonesia maupun PDPA Malaysia mengatur sejumlah hak dasar yang dimiliki oleh individu atas data pribadinya. Misalnya, hak akses diatur dalam Pasal 5 UU PDP, yang memberikan wewenang kepada subjek data untuk memperoleh informasi terkait identitas, dasar kepentingan hukum, tujuan, dan akuntabilitas pengendali data.

Pasal 5: Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi

Regulasi serupa ditemukan dalam Pasal 12 PDPA Malaysia, yang mengizinkan individu untuk mengakses dan memperoleh salinan data pribadi yang dikumpulkan oleh pengendali data.²¹

Section 12 : A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where

²⁰ Doly.

²¹ Sekaring Ayumeida Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16, <https://doi.org/10.47776/alwasath.v2i1.127>.

compliance with a request to such access or correction is refused under this Act.).

Perbedaan utama antara kedua regulasi terletak pada mekanisme pengajuan akses, di mana Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia mewajibkan prosedur yang lebih formal dibandingkan dengan *Personal Data Protection Act* (PDPA) Malaysia yang relatif lebih fleksibel. Prosedur formal tersebut ditegaskan melalui Pasal 14 UU PDP, yang mengatur bahwa pelaksanaan hak subjek data sebagaimana diatur dalam Pasal 6 sampai dengan Pasal 11 harus diajukan melalui permohonan tercatat yang disampaikan secara elektronik atau non-elektronik kepada pengendali data pribadi. Ketentuan ini, disertai dengan klausul "sesuai dengan peraturan perundang-undangan" sebagaimana termuat dalam Pasal 7²² dan Pasal 8²³, menegaskan bahwa implementasi hak subjek data di Indonesia dilaksanakan dengan standar administratif yang ketat guna memastikan transparansi, akuntabilitas, dan kepastian hukum.

Selain hak akses, kedua regulasi juga mengakui hak untuk memperbaiki atau memperbarui data pribadi. Pasal 6 UU PDP²⁴ menetapkan bahwa subjek data dapat meminta pembaruan data yang tidak akurat atau sudah kedaluwarsa, sejalan dengan prinsip keakuratan data yang menjadi bagian dari perlindungan data pribadi. Di Malaysia, hak serupa tercantum dalam Pasal 34 PDPA, yang memungkinkan individu untuk mengajukan permintaan perbaikan data secara tertulis kepada pengendali data. Namun, implementasi hak ini di Malaysia dapat dipengaruhi oleh kebijakan internal pengendali data, yang dalam beberapa kasus dapat membatasi efektivitas pelaksanaannya.²⁵ Oleh karena itu, transparansi dan akuntabilitas pengendali data menjadi faktor penting dalam menjamin efektivitas hak perbaikan data pribadi

Salah satu perbedaan signifikan antara kedua regulasi adalah terkait hak untuk menghapus data pribadi atau yang dikenal sebagai *right to be forgotten*. UU PDP Indonesia

²² Subjek Data Pribadi berhak mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.

²³ Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/ atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.

²⁴ Subjek Data Pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi

²⁵ Daniswara dan Rahman, "Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia," 10.

mengakomodasi hak ini dalam Pasal 8²⁶, memungkinkan subjek data untuk meminta penghapusan data dalam kondisi tertentu, seperti jika data tidak lagi relevan atau telah diproses secara tidak sah. Sebaliknya, PDPA Malaysia tidak secara eksplisit mengatur hak ini, sehingga permintaan penghapusan data lebih bergantung pada kebijakan masing-masing pengendali data. Hal ini menunjukkan bahwa regulasi Indonesia lebih progresif dalam memberikan perlindungan kepada subjek data dibandingkan Malaysia.

Pasal 9 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) Indonesia menyatakan bahwa subjek data pribadi berhak menarik kembali persetujuan pemrosesan data pribadinya yang telah diberikan kepada pengendali data pribadi. Selain itu, Pasal 40 ayat (1) UU PDP mengatur bahwa pengendali data pribadi wajib menghentikan pemrosesan data pribadi dalam hal subjek data pribadi menarik kembali persetujuan tersebut. Penghentian harus dilakukan paling lambat 3 x 24 jam sejak diterimanya permintaan penarikan persetujuan. Hal ini ditegaskan dalam Pasal 40 ayat 2. Di sisi lain, Personal Data Protection Act (PDPA) 2010 Malaysia tidak secara eksplisit mengatur hak individu untuk menarik kembali persetujuan atas pemrosesan data pribadinya. Namun, *General Principle* dalam PDPA menetapkan bahwa pengendali data wajib memperoleh persetujuan dari subjek data sebelum memproses data pribadi mereka. Dalam praktiknya, beberapa organisasi di Malaysia tetap mengakui hak individu untuk menarik persetujuan melalui kebijakan internal mereka, seperti yang tercantum dalam kebijakan privasi *Omniraise*.²⁷ Hal ini menunjukkan bahwa meskipun Personal Data Protection Act (PDPA) 2010 Malaysia tidak secara eksplisit mengatur hak individu untuk menarik persetujuan, beberapa perusahaan, seperti Omniraise, tetap mengakomodasi hak tersebut dalam kebijakan internal mereka.

Selain aspek hak subjek data, implementasi kebijakan perlindungan data di kedua negara juga memiliki perbedaan yang cukup mencolok. Struktur kelembagaan pengawas perlindungan data di Indonesia masih dalam tahap pembentukan, sebagaimana diamanatkan dalam Pasal 58 UU PDP. Hingga saat ini, lembaga tersebut masih menunggu keputusan Presiden untuk dapat beroperasi secara resmi. Sebaliknya, Malaysia telah lebih dahulu memiliki *Personal Data Protection Department* (JPDP) sejak 2011, yang berada di bawah Kementerian Digital. Namun, independensi JPDP masih dipertanyakan karena lembaga ini tetap berada dalam pengaruh eksekutif.

Selain perbedaan dalam struktur kelembagaan, efektivitas regulasi perlindungan data pribadi di Indonesia juga sangat bergantung pada penegakan hukum dan mekanisme

²⁶ Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/ atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan

²⁷ <https://omniraise.com/pdpa-notice/>

sanksi yang diatur secara komprehensif dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). UU PDP mengadopsi sistem sanksi administratif dan pidana yang jauh lebih tegas dibandingkan dengan Personal Data Protection Act (PDPA) 2010 di Malaysia. Sebagai contoh, Pasal 57 ayat (2) UU PDP menetapkan bahwa sanksi administratif dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data, serta denda administratif. Selanjutnya, menurut Pasal 57 ayat (3), denda administratif tersebut dapat dikenakan hingga maksimal dua persen dari pendapatan atau penerimaan tahunan, tergantung pada variabel pelanggaran.

Lebih jauh, Pasal 67 UU PDP mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya dapat dijatuhi hukuman pidana, dengan ancaman penjara hingga lima tahun dan/atau denda maksimal Rp5 miliar.²⁸ Pasal 68 menambah sanksi bagi pelaku yang membuat atau memalsukan data pribadi dengan tujuan menguntungkan diri sendiri atau orang lain, dengan ancaman penjara hingga enam tahun dan denda maksimal Rp6 miliar. Selain itu, Pasal 69 menetapkan bahwa selain hukuman utama tersebut, pelaku dapat dikenai sanksi tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh atau merupakan hasil tindak pidana, serta kewajiban untuk membayar ganti kerugian.

Dalam konteks korporasi, Pasal 70 UU PDP mengatur bahwa apabila tindak pidana dilakukan oleh suatu korporasi, sanksi pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, atau pemilik manfaat, serta kepada korporasi itu sendiri,²⁹ yang dikenai denda administratif hingga sepuluh kali dari denda yang diancamkan.³⁰ Sanksi tambahan bagi korporasi juga mencakup perampasan keuntungan, pembekuan usaha, pencabutan izin, dan bahkan pembubaran korporasi.³¹

Lebih lanjut, Pasal 71 UU PDP mengatur mekanisme pembayaran denda, yang mengharuskan terpidana melunasi denda dalam jangka waktu satu bulan sejak putusan memperoleh kekuatan hukum tetap³², dengan kemungkinan perpanjangan maksimal satu bulan apabila terdapat alasan kuat³³. Apabila denda tidak dilunasi, harta kekayaan atau pendapatan terpidana dapat disita dan dilelang³⁴, atau jika penyitaan tidak mencukupi,

²⁸ Indah Alvi Wardani dan Deaf Wahyuni Ramadhani, "STUDI PERBANDINGAN TENTANG TINDAK PIDANA DOXING DI INDONESIA, MALAYSIA, SINGAPURA, DAN THAILAND," 2024, Universitas Bung Hatta.

²⁹ Pasal 70 ayat 1

³⁰ Pasal 70 ayat 3

³¹ Pasal 70 ayat 4

³² Pasal 71 ayat 1

³³ Pasal 71 ayat 2

³⁴ Pasal 71 ayat 3

denda tersebut akan diganti dengan pidana penjara sesuai ketentuan yang ditetapkan hakim³⁵.

Sebaliknya, PDPA 2010 Malaysia hanya menetapkan sanksi administratif dengan denda maksimal sebesar RM 500.000³⁶, mencerminkan pendekatan penegakan hukum yang lebih ringan. Perbedaan dalam mekanisme sanksi ini menegaskan bahwa Indonesia berupaya menerapkan standar perlindungan data pribadi yang lebih ketat melalui kerangka sanksi yang komprehensif, sehingga diharapkan dapat menimbulkan efek jera yang lebih kuat terhadap para pelanggar.

Dari perspektif cakupan regulasi, UU PDP Indonesia memiliki keunggulan karena bersifat menyeluruh, di mana Pasal 2 menetapkan bahwa undang-undang ini berlaku bagi setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum di wilayah hukum Indonesia atau yang menimbulkan akibat hukum di Indonesia, termasuk pengolahan data pribadi di sektor publik maupun swasta. Sebaliknya, PDPA Malaysia hanya mengatur pemrosesan data pribadi dalam konteks transaksi komersial sebagaimana diatur dalam Pasal 3(1) PDPA 2010, sehingga sektor publik tidak termasuk dalam cakupannya. Pembatasan ini berpotensi menciptakan celah dalam perlindungan data pribadi warga negara, sehingga menimbulkan tantangan dalam memastikan standar perlindungan data yang komprehensif di Malaysia.

Dalam konteks kerja sama internasional, perbedaan pendekatan regulasi terkait transfer data lintas negara antara Indonesia dan Malaysia terletak pada ketentuan yang mengatur persyaratan perlindungan data. Berdasarkan UU PDP Indonesia, khususnya Pasal 56 ayat (1)–(5), transfer Data Pribadi ke luar negeri hanya diperbolehkan apabila negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi dari standar yang ditetapkan. Apabila ketentuan tersebut tidak terpenuhi, pengendali data diwajibkan memastikan adanya perlindungan data yang memadai dan bersifat mengikat, atau memperoleh persetujuan dari subjek data, sebagaimana diatur dalam Pasal 56 ayat (4).³⁷ Sebaliknya, PDPA 2010 Malaysia melalui Pasal 129 mengharuskan setiap transfer data pribadi ke luar negeri untuk mendapatkan persetujuan dari Menteri.³⁸ Namun, hingga saat ini, daftar negara yang secara resmi memenuhi kriteria tersebut belum ditetapkan, sehingga penerapan kebijakan ini masih terbatas secara praktis. Perbedaan ini menunjukkan bahwa

³⁵ Pasal 71 ayat 4

³⁶ Rizal, “Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia,” 223.

³⁷ Fanisa Mayda Ayiliani dan Elfia Farida, “Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara,” *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–33.

³⁸ PDPA, “Laws of Malaysia Act 709 Personal Data Protection Act 2010,” *10 June 2010*, no. 2 (2010): 95, [http://www.kkmm.gov.my/pdf/Personal Data Protection Act 2010.pdf](http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf).

kerangka regulasi di Indonesia lebih komprehensif dalam menjamin perlindungan data lintas negara, sedangkan pendekatan di Malaysia cenderung lebih sempit karena hanya mengatur transaksi komersial.

Secara keseluruhan, baik Indonesia maupun Malaysia telah mengadopsi kebijakan perlindungan data pribadi yang mengatur hak subjek data dan mekanisme pengawasannya.³⁹ Namun, terdapat beberapa perbedaan mendasar dalam cakupan, penegakan hukum, serta independensi otoritas pengawas. UU PDP Indonesia memiliki pendekatan yang lebih luas dan sanksi yang lebih ketat dibandingkan PDPA Malaysia, yang lebih terbatas dalam yurisdiksinya. Oleh karena itu, efektivitas perlindungan data di kedua negara sangat bergantung pada implementasi kebijakan yang lebih komprehensif dan transparan untuk memastikan hak subjek data benar-benar terlindungi sesuai dengan standar global.

4. Kesimpulan

Penelitian ini mengungkapkan bahwa meskipun Indonesia dan Malaysia sama-sama telah mengadopsi regulasi perlindungan data pribadi, terdapat perbedaan mendasar dalam cakupan hukum, mekanisme pelaksanaan hak subjek data, struktur kelembagaan, serta penegakan hukum. UU PDP Indonesia menampilkan pendekatan yang lebih komprehensif dan ketat, mencakup seluruh sektor—publik maupun swasta—serta menerapkan prosedur formal untuk akses, koreksi, penghapusan, dan penarikan persetujuan, yang disertai dengan sanksi administratif dan pidana yang signifikan. Sebaliknya, PDPA 2010 di Malaysia, yang hanya berlaku untuk transaksi komersial, tidak mengatur sektor publik dan mengandalkan sanksi administratif dengan denda maksimal yang relatif rendah, sehingga menciptakan celah dalam perlindungan data dan menimbulkan tantangan dalam efektivitas penegakan hukum.

Implikasi praktis dari perbandingan ini menunjukkan bahwa Indonesia memiliki potensi untuk mengembangkan standar perlindungan data pribadi yang lebih menyeluruh, asalkan diiringi dengan reformasi kelembagaan yang meningkatkan independensi otoritas pengawas dan penegakan hukum yang konsisten. Penelitian ini, dengan pendekatan normatif dan perbandingan hukum, memberikan dasar analisis yang kuat untuk menilai perbedaan antara kedua sistem regulasi dan menyarankan bahwa penyesuaian kerangka hukum, termasuk adopsi prinsip-prinsip GDPR, sangat penting bagi pembuat kebijakan di

³⁹ Ninuk Triyanti et al., “Hasanuddin LawReview Legal Gaps in Personal Data Protection: Reforming Indonesia’s Population Administration Law,” *HasanuddinLawReview* 1, no. 1 (2025): 132–47, <https://doi.org/10.20956/halrev.v1i1.6177>.

kedua negara guna meningkatkan transparansi, akuntabilitas, dan kepastian hukum dalam perlindungan data pribadi.

5. Daftar Pustaka

- Ahdiat, Adi. "Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar." <https://databoks.katadata.co.id>, 2024. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>.
- Alibeigi, Ali, dan Abu Bakar Munir. "Malaysian personal data protection act, a mysterious application." *University of Bologna Law Review* 5, no. 2 (2020): 362–74. <https://doi.org/10.6092/ISSN.2531-6133/12441>.
- Ayiliani, Fanisa Mayda, dan Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–33.
- Daniswara, Fahreza, dan Faiz Rahman. "Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia." *Center For Digital Society* 31 (2018): 24.
- Djafar, Wahyudi, dan M. Jodi Santoso. *PERLINDUNGAN DATA PRIBADI: Pentingnya Otoritas Pengawasan Independen. Lembaga Studi dan Advokasi Masyarakat (ELSAM)*, 2019.
- Doly, Denico. "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru." *Negara Hukum* 12, no. 2 (2021): 227.
- Dwi, Andika. "10 Negara dengan Kasus Kebocoran Data Terbanyak, Mirip PDN Indonesia." *Tempo.co*, 2024.
- Fachri, Ferinda K. "Deputi BSSN: Penyebab Kebocoran Data Pribadi Biasanya Kepatuhan Hukum yang Kurang." *Hukum Online*, 2024. <https://www.hukumonline.com/berita/a/deputi-bssn--penyebab-kebocoran-data-pribadi-biasanya-kepatuhan-hukum-yang-kurang-lt6644ead0802f8/?page=2>.
- Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data)." In *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 43–60, 2020. <http://jurnal.unissula.ac.id/index.php/PH/article/view/1476>.
- Intan, Ghita. "Pusat Data Nasional Diretas, Pakar: Pemerintah Tak Pernah Belajar dari Kesalahan." *VOA Indonesia.com*, 2024, 1–5. <https://www.voaindonesia.com/a/pusat-data-nasional-diretas-pakar-pemerintah-tak-pernah-belajar-dari-kesalahan/7682298.html>.
- Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>.

- Matheus, Juan, dan Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *Justisi* 10, no. 1 (2023): 20–35. <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.
- Mustafa, Irfan Amir, Asni Zubair, dan Hamzah Hamzah. *Kampus Merdeka. CV Bintang Semesta Media*. Yogyakarta: Bintang Semesta Media, 2023.
- PDPA. "Laws of Malaysia Act 709 Personal Data Protection Act 2010." *10 June 2010*, no. 2 (2010): 95. [http://www.kkmm.gov.my/pdf/Personal Data Protection Act 2010.pdf](http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf).
- Razaq, Niken. "11 Kasus Kebocoran Data di Malaysia Dua Tahun Terakhir." *cyberthreat.id*, 2023. <https://cyberthreat.id/read/15129/11-Kasus-Kebocoran-Data-di-Malaysia-Dua-Tahun-Terakhir>.
- Rizal, Muhammad Saiful. "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia." *Jurnal Cakrawala Hukum* 10, no. 2 (2019): 218–27. <https://doi.org/10.26905/idjch.v10i2.3349>.
- Rizki, Mochamad Januar. "Menyorot Independensi Lembaga Pengawas Data Pribadi." *Hukum Online.com*, 2023. <https://www.hukumonline.com/berita/a/menyorot-independensi-lembaga-pengawas-data-pribadi-lt6461f9e088aeb>.
- Roy Franedy. "91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M." *CNBC Indonesia*, 2020, 1–5.
- Singgih, Viriya. "Petinggi Kominfo mundur 'sebagai tanggung jawab moral' setelah Pusat Data Nasional diretas." *BBC News Indonesia*, 2024, 1–21. <https://www.bbc.com/indonesia/articles/c8vdmymmyzo>.
- Triyanti, Ninuk, I Gusti Ayu, Ketut Rachmi, dan Lego Karjoko. "Hasanuddin LawReview Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law." *HasanuddinLawReview* 1, no. 1 (2025): 132–47. <https://doi.org/10.20956/halrev.v1i1.6177>.
- Wardani, Indah Alvi, dan Deaf Wahyuni Ramadhani. "STUDI PERBANDINGAN TENTANG TINDAK PIDANA DOXING DI INDONESIA, MALAYSIA, SINGAPURA, DAN THAILAND," 2024. Universitas Bung Hatta.
- Widjaja, Gunawan, dan Fransiska Milenia Cesarianti. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *SINERGI: Jurnal Riset Ilmiah* 1, no. 4 (2024): 234–42. <https://doi.org/10.62335/8qf44b59>.