

Harmonisasi Hukum Pelindungan Data Pribadi di Indonesia dan Singapura dalam Kerangka *Asia-Pacific Economic Cooperation Privacy Framework*

Chariestine Vanessa ^{a, 1}, David Tan ^{a, 2*}, Agustianto ^{a, 3}

^a Universitas Internasional Batam, Indonesia

² david.tan@uib.ac.id*

*korespondensi penulis

Informasi artikel

Received: 20 Juni 2026;

Revised: 27 Juni 2026;

Accepted: 8 Agustus 2026.

Kata-kata kunci:

Pelindungan Data Pribadi;

Perusahaan Digital;

Harmonisasi Hukum;

APEC Privacy

Framework;

Interoperabilitas.

: ABSTRAK

Pesatnya perkembangan perusahaan digital telah meningkatkan pengolahan data pribadi sekaligus menimbulkan tantangan pelindungan data dalam aktivitas ekonomi digital lintas batas. Penelitian ini bertujuan menganalisis pengaturan pelindungan data pribadi bagi perusahaan digital di Indonesia dan Singapura serta mengkaji arah harmonisasinya berdasarkan Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, perbandingan, dan konseptual melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa Indonesia dan Singapura telah mengadopsi prinsip-prinsip pelindungan data yang sejalan dengan APEC Privacy Framework, namun berbeda dalam efektivitas implementasi, kapasitas kelembagaan, dan mekanisme pengawasan. Indonesia masih menghadapi tantangan dalam penegakan hukum, pengawasan, dan kepatuhan organisasi, sedangkan Singapura menunjukkan implementasi yang lebih operasional melalui penguatan mekanisme *accountability* dan peran aktif Personal Data Protection Commission (PDPC). Penelitian ini menemukan bahwa harmonisasi pengaturan pelindungan data pribadi paling tepat dilakukan melalui model interoperabilitas sebagaimana dikembangkan dalam APEC Privacy Framework, sehingga mendukung penyelarasan standar pelindungan data tanpa menghilangkan karakteristik sistem hukum nasional masing-masing negara.

ABSTRACT

Keywords:

Personal Data Protection;

Digital Companies;

Legal Harmonization;

APEC Privacy

Framework;

Interoperability.

Legal Harmonization of Personal Data Protection in Indonesia and Singapore within the APEC Privacy Framework. The rapid growth of digital companies has intensified the processing of personal data while creating greater challenges for personal data protection in cross-border digital economic activities. This study aims to analyze the regulation of personal data protection for digital companies in Indonesia and Singapore and to examine the direction of legal harmonization based on the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. This study employs normative legal research using statutory, comparative, and conceptual approaches through library research. The findings indicate that Indonesia and Singapore have adopted personal data protection principles consistent with the APEC Privacy Framework but differ in implementation effectiveness, institutional capacity, and supervisory mechanisms. Indonesia continues to face challenges related to law enforcement, regulatory oversight, and organizational compliance, whereas Singapore demonstrates a more operational approach through stronger accountability mechanisms and the active role of the Personal Data Protection Commission (PDPC). The study finds that harmonization should adopt an interoperability model under the APEC Privacy Framework, enabling the alignment of personal data protection standards while preserving the characteristics of each national legal system.

Copyright © 2026 (Chariestine Vanessa, dkk). All Right Reserved

How to Cite : Vanessa, C., Tan, D., & Agustianto, A. (2026). Harmonisasi Hukum Pelindungan Data Pribadi di Indonesia dan Singapura dalam Kerangka Asia-Pacific Economic Cooperation Privacy Framework. *Nomos : Jurnal Penelitian Ilmu Hukum*, 6(1), 84–101.
<https://doi.org/10.56393/nomos.v6i1.4578>



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/). Allows readers to read, download, copy, distribute, print, search, or link to the full texts of its articles and allow readers to use them for any other lawful purpose. The journal hold the copyright.

Pendahuluan

Perkembangan ekonomi digital di kawasan Asia Tenggara dalam satu dekade terakhir menunjukkan pertumbuhan yang sangat pesat. Indonesia bahkan diproyeksikan menjadi pasar ekonomi digital terbesar di kawasan dengan nilai mencapai USD130 miliar pada tahun 2025, seiring meningkatnya aktivitas perusahaan digital (*startup*) di sektor *e-commerce*, *financial technology* (*fintech*), *education technology* (*edutech*), dan *health technology* (*healthtech*) yang sangat bergantung pada pemrosesan data pribadi pengguna (Google, Temasek, & Bain, 2022). Laporan e-Conomy SEA 2024 menunjukkan bahwa ekonomi digital Asia Tenggara terus mengalami pertumbuhan yang didorong oleh peningkatan transaksi digital dan ekspansi ekosistem *startup* di berbagai sektor ekonomi (Google, Temasek, & Bain, 2024). Namun, kemajuan ini menimbulkan persoalan baru terkait keamanan dan pelindungan data pribadi, mengingat *Cost of a Data Breach Report 2024* menunjukkan bahwa kebocoran data masih menjadi ancaman serius dengan dampak ekonomi yang terus meningkat bagi organisasi di berbagai negara (IBM, 2024). Fenomena ini tersebut menunjukkan bahwa pelindungan data pribadi tidak lagi hanya menjadi persoalan teknis, tetapi telah berkembang menjadi isu hukum yang memerlukan kepastian hukum, pengawasan, dan mekanisme pertanggungjawaban yang efektif.

Isu pelindungan data pribadi tidak hanya menjadi perhatian nasional, tetapi juga telah berkembang menjadi isu hukum global. United Nations Conference on Trade and Development (UNCTAD) mencatat bahwa lebih dari 137 negara telah memiliki regulasi pelindungan data pribadi (UNCTAD, 2021). Di tingkat internasional, General Data Protection Regulation (GDPR) dari Uni Eropa dan California Consumer Privacy Act (CCPA) dari Amerika Serikat sering dijadikan acuan dalam pengembangan regulasi pelindungan data pribadi karena memiliki standar yang relatif komprehensif. Selain itu, perkembangan tata kelola digital di kawasan Asia Tenggara juga didorong melalui berbagai inisiatif regional yang menekankan interoperabilitas dan kerja sama lintas negara dalam pengelolaan data digital. Sementara itu, di kawasan Asia-Pasifik, Asia-Pacific Economic Cooperation (APEC) Privacy Framework hadir sebagai pedoman bagi negara-negara anggotanya dengan menekankan prinsip transparansi, akuntabilitas, keamanan data, dan pelindungan data lintas batas (*cross-border privacy protection*) (APEC, 2015). Berbeda dengan GDPR yang memiliki kekuatan mengikat (*hard law*), APEC Privacy Framework merupakan instrumen *soft law* yang memberikan fleksibilitas bagi negara anggota dalam menyusun kebijakan nasional sekaligus mendorong interoperabilitas pelindungan data di kawasan Asia-Pasifik. Menurut Rosadi (2018), harmonisasi pengaturan pelindungan data pribadi tidak hanya bertujuan menciptakan kepastian hukum bagi pelaku usaha digital, tetapi juga menjamin perlindungan hak privasi sebagai bagian dari hak asasi manusia dalam perkembangan ekonomi digital.

Dalam konteks Indonesia, pengaturan pelindungan data pribadi secara komprehensif baru diwujudkan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP, 2022). Secara normatif (*das sollen*), UU PDP telah mengatur hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data pribadi, serta amanat pembentukan otoritas pelindungan data pribadi sebagaimana diatur dalam Pasal 58 ayat (3), Pasal 59, dan Pasal 60 UU PDP. Namun, dalam praktik (*das sein*), implementasi pengaturan tersebut masih menghadapi berbagai kendala. Sejumlah kajian menunjukkan bahwa sebagian perusahaan digital belum sepenuhnya memenuhi kewajiban pelindungan data pribadi, termasuk belum optimalnya penunjukan *data protection officer*, mekanisme pelaporan insiden kebocoran data, serta penerapan tata kelola data yang sesuai dengan ketentuan peraturan perundang-undangan (Azmi & Sanjaya, 2023; Razi et al., 2024). Sejalan dengan kondisi tersebut, perbedaan antara pengaturan normatif dan implementasi empiris tersebut menunjukkan pentingnya melakukan analisis terhadap efektivitas pelindungan data pribadi di Indonesia

melalui perbandingan dengan Singapura sebagai negara yang telah memiliki sistem pengawasan dan penegakan hukum yang lebih matang melalui Personal Data Protection Commission (PDPC).

Penelitian mengenai pelindungan data pribadi telah berkembang dari berbagai perspektif, baik yang berfokus pada regulasi nasional, implementasi kebijakan, maupun kerangka pelindungan data di tingkat internasional. Dalam konteks Indonesia, Razi et al. (2024) menemukan bahwa pelindungan data pribadi masih menghadapi berbagai kendala akibat belum adanya regulasi yang komprehensif sehingga perlindungan terhadap hak subjek data belum berjalan secara optimal. Setelah berlakunya UU PDP, Syailendra (2023) menunjukkan bahwa tantangan pelindungan data pribadi bergeser dari pembentukan regulasi menuju efektivitas implementasi, khususnya dalam pemenuhan kewajiban oleh pengendali data dan mekanisme penegakan hukumnya. Kedua penelitian tersebut menggambarkan perkembangan rezim pelindungan data pribadi di Indonesia, namun masih berfokus pada konteks nasional tanpa melakukan analisis komparatif dengan negara lain. Sementara itu, Personal Data Protection Commission, (2022) menjelaskan bahwa penerapan Personal Data Protection Act (PDPA) di Singapura didukung oleh pengawasan kelembagaan yang aktif sehingga mampu meningkatkan kepatuhan organisasi terhadap kewajiban pelindungan data pribadi. Pada tingkat internasional, APEC (2015) menetapkan prinsip-prinsip pelindungan data lintas batas (*cross-border privacy protection*) serta *accountability* sebagai pedoman bagi negara anggota, tetapi tidak memberikan mekanisme implementasi yang mengikat karena bersifat *soft law*. Wu (2024) menekankan pentingnya menjaga keseimbangan antara inovasi digital dan pelindungan hak privasi konsumen. Di sisi lain, Riyadi (2021) dan Suleiman (2022) masih menggunakan GDPR sebagai acuan utama dalam mengevaluasi regulasi pelindungan data pribadi di Indonesia, sementara penelitian mengenai kesadaran masyarakat menunjukkan bahwa efektivitas pelindungan data pribadi juga dipengaruhi oleh rendahnya pemahaman publik terhadap hak atas privasi data (IJSSHR, 2024). Secara keseluruhan, penelitian-penelitian terdahulu telah memberikan kontribusi penting dalam menjelaskan perkembangan regulasi dan implementasi pelindungan data pribadi. Namun, kajian tersebut masih cenderung dilakukan secara parsial, baik yang berfokus pada regulasi nasional, praktik implementasi di satu negara, maupun prinsip-prinsip pelindungan data di tingkat internasional, sehingga belum memberikan analisis yang terintegrasi mengenai harmonisasi pengaturan pelindungan data pribadi di kawasan Asia-Pasifik.

Kebaruan (*novelty*) penelitian ini terletak pada penggunaan APEC Privacy Framework sebagai kerangka analisis utama untuk mengevaluasi kesesuaian pengaturan pelindungan data pribadi di Indonesia dan Singapura serta merumuskan arah harmonisasi hukumnya. Berbeda dengan penelitian-penelitian terdahulu yang umumnya berfokus pada implementasi regulasi nasional, menggunakan GDPR sebagai standar pembandingan, atau hanya membahas prinsip-prinsip pelindungan data secara normatif, penelitian ini mengintegrasikan tiga aspek sekaligus, yaitu analisis komparatif antara Indonesia dan Singapura, evaluasi terhadap efektivitas implementasi pengaturan pelindungan data pribadi, serta penilaian kesesuaiannya berdasarkan prinsip-prinsip APEC Privacy Framework dalam konteks perusahaan digital (*startup*). Dengan mempertimbangkan hal tersebut, penelitian ini tidak hanya menghasilkan perbandingan regulasi kedua negara, tetapi juga menawarkan perspektif mengenai model harmonisasi hukum pelindungan data pribadi yang lebih adaptif terhadap karakteristik ekonomi digital dan tata kelola data lintas batas di kawasan Asia-Pasifik.

Penelitian ini memberikan kontribusi secara teoretis maupun praktis dalam pengembangan hukum pelindungan data pribadi. Secara teoretis, penelitian ini memperkaya kajian hukum komparatif mengenai pelindungan data pribadi melalui analisis kesesuaian pengaturan di Indonesia dan Singapura dengan menggunakan APEC Privacy Framework sebagai kerangka harmonisasi hukum di kawasan Asia-Pasifik. Kontribusi tersebut diharapkan dapat memperluas pengembangan literatur mengenai harmonisasi pelindungan data pribadi, khususnya dalam konteks perusahaan digital (*startup*) yang melakukan pemrosesan data lintas batas. Secara praktis, hasil penelitian ini memberikan rekomendasi

bagi pembentuk kebijakan, regulator, dan pelaku usaha digital dalam memperkuat implementasi Undang-Undang Pelindungan Data Pribadi serta mendorong penyusunan kebijakan yang lebih adaptif terhadap tata kelola data lintas negara. Selain itu, penelitian ini juga memberikan kontribusi terhadap pengembangan hukum Indonesia (*ius constituendum*) melalui rekomendasi arah harmonisasi pelindungan data pribadi yang selaras dengan prinsip-prinsip APEC Privacy Framework tanpa mengesampingkan karakteristik sistem hukum nasional. Meskipun demikian, penelitian ini masih memiliki keterbatasan karena hanya membandingkan pengaturan pelindungan data pribadi di Indonesia dan Singapura dengan pendekatan penelitian hukum normatif, sehingga belum mencakup analisis empiris mengenai efektivitas implementasi regulasi di tingkat organisasi maupun masyarakat. Keterbatasan tersebut diharapkan dapat menjadi ruang bagi penelitian selanjutnya untuk mengembangkan kajian yang lebih komprehensif.

Berdasarkan latar belakang, penelitian terdahulu, serta *research gap* yang telah diuraikan, penelitian ini diarahkan untuk menjawab dua pertanyaan penelitian. Pertama, kesesuaian pengaturan pelindungan data pribadi bagi perusahaan digital (*startup*) di Indonesia dan Singapura berdasarkan prinsip-prinsip APEC Privacy Framework dan arah harmonisasi pengaturan pelindungan data pribadi di Indonesia dan Singapura berdasarkan hasil analisis terhadap prinsip-prinsip APEC Privacy Framework, kedua pertanyaan tersebut menjadi landasan dalam mengevaluasi kesesuaian pengaturan yang berlaku sekaligus merumuskan arah harmonisasi hukum pelindungan data pribadi yang lebih adaptif terhadap perkembangan ekonomi digital di kawasan Asia-Pasifik. Berdasarkan pertanyaan penelitian tersebut, penelitian ini bertujuan untuk menganalisis kesesuaian pengaturan pelindungan data pribadi bagi perusahaan digital (*startup*) di Indonesia dan Singapura berdasarkan prinsip-prinsip APEC Privacy Framework. Selain itu, penelitian ini juga bertujuan untuk menganalisis arah harmonisasi pengaturan pelindungan data pribadi di kedua negara berdasarkan hasil analisis komparatif yang dilakukan. Melalui pencapaian tujuan tersebut, penelitian ini diharapkan dapat memberikan rekomendasi konseptual mengenai model harmonisasi pelindungan data pribadi yang lebih adaptif terhadap perkembangan ekonomi digital serta memperkuat pengembangan hukum pelindungan data pribadi di kawasan Asia-Pasifik.

Metode

Penelitian ini menggunakan metode penelitian hukum normatif dengan studi kepustakaan (*library research*) yang berfokus pada pengkajian norma hukum melalui peraturan perundang-undangan, doktrin, dan literatur ilmiah (Disemadi, 2022; Tan, 2021). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan perbandingan (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk mengkaji regulasi pelindungan data pribadi di Indonesia dan Singapura, sedangkan pendekatan perbandingan diterapkan untuk mengidentifikasi persamaan, perbedaan, serta keunggulan pengaturan kedua negara berdasarkan parameter yang sama. Adapun pendekatan konseptual digunakan untuk menganalisis kesesuaian pengaturan tersebut dengan prinsip-prinsip *APEC Privacy Framework* sebagai dasar perumusan arah harmonisasi hukum. Bahan hukum yang dianalisis terdiri atas bahan hukum primer berupa peraturan perundang-undangan yang relevan, bahan hukum sekunder berupa buku, artikel jurnal ilmiah, hasil penelitian, dan dokumen resmi, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia. Singapura dipilih sebagai negara pembanding karena memiliki rezim pelindungan data pribadi yang relatif lebih matang, berada dalam kawasan ekonomi digital yang sama dengan Indonesia, dan merupakan anggota APEC sehingga relevan dengan kerangka analisis yang digunakan. Analisis dilakukan secara kualitatif melalui tahapan reduksi, klasifikasi, dan interpretasi bahan hukum, kemudian dilanjutkan dengan analisis komparatif berdasarkan aspek ruang lingkup pelindungan data, hak subjek data, kewajiban pengendali data, transfer data lintas batas, kelembagaan pengawas, dan mekanisme penegakan hukum. Keabsahan analisis dijaga melalui penggunaan sumber

hukum yang otoritatif dan masih berlaku serta triangulasi antara bahan hukum primer dan sekunder, sedangkan penarikan kesimpulan dilakukan secara deduktif untuk merumuskan rekomendasi pengembangan hukum (*ius constituendum*) mengenai harmonisasi pelindungan data pribadi di Indonesia berdasarkan prinsip-prinsip *APEC Privacy Framework*.

Hasil dan Pembahasan

Perkembangan perusahaan digital (*startup*) telah meningkatkan intensitas pengolahan data pribadi, termasuk melalui aktivitas pemrosesan data lintas batas yang menimbulkan tantangan hukum baru. Oleh karena itu, pengaturan pelindungan data pribadi menjadi aspek yang penting untuk menjamin perlindungan hak individu sekaligus memberikan kepastian hukum bagi pelaku usaha digital. Berdasarkan hasil penelitian, Indonesia dan Singapura memiliki pendekatan yang berbeda dalam mengatur pelindungan data pribadi. Indonesia cenderung menerapkan pendekatan yang lebih normatif melalui UU PDP, sedangkan Singapura mengedepankan pendekatan yang lebih adaptif melalui PDPA. Perbedaan tersebut menjadi dasar untuk menganalisis tingkat kesesuaian pengaturan kedua negara berdasarkan prinsip-prinsip dalam *APEC Privacy Framework*.

Berdasarkan hasil penelitian, pengaturan mengenai definisi data pribadi di Indonesia dan Singapura menunjukkan persamaan dalam mengakui bahwa data pribadi merupakan setiap informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Sejalan dengan kondisi tersebut, kedua negara menerapkan pendekatan yang berbeda dalam merumuskan definisi tersebut. UU PDP mengatur data pribadi secara lebih rinci melalui pengelompokan data pribadi umum dan data pribadi spesifik, sehingga mencerminkan pendekatan berbasis klasifikasi dan tingkat risiko. Sebaliknya, PDPA Singapura mendefinisikan data pribadi secara lebih fungsional dengan menitikberatkan pada hubungan antara data, organisasi sebagai pengendali data, dan tujuan penggunaannya dalam kegiatan bisnis. Perbedaan tersebut menunjukkan bahwa Indonesia lebih menekankan kepastian normatif melalui pengaturan yang terperinci, sedangkan Singapura lebih mengutamakan fleksibilitas dalam implementasi pengelolaan data oleh organisasi. Secara konseptual, kedua pendekatan tersebut tetap sejalan dengan pandangan Kuner (2017) yang menyatakan bahwa data pribadi mencakup seluruh informasi yang mampu mengidentifikasi individu secara langsung maupun tidak langsung. Namun, perkembangan teknologi digital yang ditandai dengan pemanfaatan *big data*, kecerdasan buatan, dan analisis perilaku pengguna menyebabkan batas antara data pribadi dan data non-pribadi semakin sulit dibedakan sebagaimana dikemukakan oleh Wu (2024). Kondisi tersebut menunjukkan bahwa definisi data pribadi tidak lagi hanya dipahami sebagai konsep normatif, tetapi juga harus mampu mengakomodasi perkembangan teknologi dan model bisnis digital yang terus berkembang.

Tabel 1. Perbandingan Pengaturan Definisi Data Pribadi di Indonesia dan Singapura

Aspek	Indonesia (UU PDP)	Singapura (PDPA)
Definisi data pribadi	Pasal 1 angka 1 – Data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung.	Section 2(1) – Personal data means data, whether true or not, about an individual who can be identified.
Prinsip pengolahan data	Pasal 16–19 – Mengatur prinsip pemrosesan data, termasuk tujuan tertentu, akurasi, pembatasan pemrosesan, dan keamanan data.	Sections 13–18, 23–24 – Mengatur consent obligation, purpose limitation, accuracy, protection, dan retention obligation.
Hak subjek data	Pasal 5–16 – Hak memperoleh informasi, akses, perbaikan, penghapusan, penarikan persetujuan, keberatan, dan hak lainnya.	Sections 21–22 serta ketentuan terkait withdrawal of consent pada Section 16 – Hak akses, koreksi, dan penarikan persetujuan.
Kewajiban pengendali data	Pasal 20–56 UU PDP, didukung UU ITE dan PP No. 71 Tahun 2019 mengenai keamanan penyelenggaraan sistem elektronik.	Sections 11–26D PDPA – Kewajiban organisasi, penunjukan DPO, perlindungan data, pelaporan pelanggaran data, dan mekanisme kepatuhan.

Transfer data lintas batas	Pasal 56 – Transfer data dilakukan dengan memperhatikan tingkat pelindungan data dan ketentuan peraturan perundang-undangan.	Section 26 – Transfer data ke luar Singapura hanya diperbolehkan apabila terdapat standar pelindungan yang sebanding.
Otoritas pengawas	Pasal 58–60 – Mengatur pembentukan lembaga pelindungan data pribadi.	Part VI PDPA – Personal Data Protection Commission (PDPC) sebagai otoritas pengawas.
Penegakan hukum dan sanksi	Pasal 57 serta Bab XIII UU PDP – Mengatur sanksi administratif dan pidana.	Parts IX–IXA PDPA – Mengatur kewenangan PDPC, denda administratif, dan mekanisme penegakan hukum.

Sebagaimana ditunjukkan pada Tabel 1, Indonesia dan Singapura pada dasarnya telah mengatur aspek-aspek utama pelindungan data pribadi, meliputi definisi data pribadi, prinsip pengolahan data, hak subjek data, kewajiban pengendali data, mekanisme transfer data lintas batas, kelembagaan pengawas, serta penegakan hukum. Meskipun kedua negara memiliki ruang lingkup pengaturan yang relatif sebanding, terdapat perbedaan dalam pendekatan regulasi dan implementasinya. Indonesia cenderung membangun kepastian hukum melalui pengaturan yang lebih rinci, sedangkan Singapura lebih menekankan mekanisme kepatuhan organisasi dan pengawasan yang adaptif. Indonesia telah memiliki kerangka regulasi yang relatif komprehensif melalui UU PDP, namun efektivitas implementasinya masih dipengaruhi oleh tantangan dalam mekanisme penegakan hukum, kelembagaan, dan kesiapan menghadapi perkembangan teknologi digital (Judijanto et al., 2024). Dalam perspektif Teori Hukum Responsif yang dikemukakan oleh Nonet dan Selznick, hukum tidak hanya dipandang sebagai seperangkat aturan yang memberikan kepastian hukum, tetapi juga sebagai instrumen yang mampu menyesuaikan diri dengan perkembangan masyarakat dan kebutuhan sosial. Oleh karena itu, perbandingan pengaturan pelindungan data pribadi di Indonesia dan Singapura tidak hanya diarahkan untuk mengidentifikasi persamaan maupun perbedaannya secara normatif, tetapi juga untuk menilai sejauh mana masing-masing sistem hukum mampu merespons perkembangan ekonomi digital, kemajuan teknologi, serta kebutuhan tata kelola data lintas batas. Berdasarkan kerangka tersebut, analisis selanjutnya dilakukan dengan mengacu pada prinsip-prinsip dalam APEC Privacy Framework sebagai parameter untuk menilai tingkat kesesuaian pengaturan kedua negara sekaligus merumuskan arah harmonisasi pelindungan data pribadi.

Berdasarkan hasil penelitian, Indonesia dan Singapura sama-sama mengatur prinsip-prinsip dasar dalam pengolahan data pribadi sebagai landasan bagi pemrosesan data yang sah dan bertanggung jawab. UU PDP mengatur prinsip keabsahan dan transparansi, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, serta integritas dan kerahasiaan data. Sementara itu, PDPA Singapura mengadopsi prinsip-prinsip yang sepadan, namun lebih menitikberatkan pada tanggung jawab organisasi dalam memastikan kepatuhan melalui mekanisme internal, seperti penyusunan kebijakan pelindungan data, penunjukan *Data Protection Officer*, serta pengawasan terhadap aktivitas pemrosesan data. Pendekatan tersebut mencerminkan konsep *accountability*, yaitu kewajiban organisasi untuk tidak hanya mematuhi ketentuan hukum, tetapi juga mampu menunjukkan dan mempertanggungjawabkan kepatuhan tersebut melalui sistem tata kelola yang efektif (Badriah et al., 2023; Hanisch et al., 2023). Perbandingan tersebut menunjukkan bahwa Indonesia lebih menekankan pemenuhan norma hukum sebagai dasar pengolahan data pribadi, sedangkan Singapura lebih berorientasi pada efektivitas implementasi melalui tata kelola organisasi. Secara konseptual, kedua pendekatan tersebut tetap sejalan dengan OECD Privacy Framework yang menempatkan pembatasan tujuan, kualitas data, dan keamanan informasi sebagai prinsip utama dalam pelindungan data pribadi (OECD, 2013). Selain itu Lynskey (2024) menjelaskan bahwa perkembangan regulasi pelindungan data modern tidak lagi hanya menitikberatkan pada keberadaan norma hukum, tetapi juga pada efektivitas mekanisme implementasi dalam menjamin pelindungan hak individu. Dalam konteks tersebut, meskipun Indonesia dan Singapura mengadopsi prinsip-prinsip pengolahan data yang relatif serupa,

keduanya menunjukkan orientasi implementasi yang berbeda, di mana Indonesia lebih berfokus pada kepastian normatif, sedangkan Singapura lebih menekankan penguatan tata kelola organisasi sebagai bentuk penerapan prinsip *accountability*.

Namun demikian, dalam konteks perusahaan digital (*startup*), penerapan prinsip-prinsip tersebut menghadapi tantangan yang signifikan. Praktik pengumpulan data secara masif, penggunaan data untuk berbagai tujuan, serta penyimpanan data dalam jangka panjang seringkali bertentangan dengan prinsip pembatasan tujuan dan minimalisasi data (Wu, 2024). Secara komparatif, Indonesia telah mengadopsi prinsip yang komprehensif secara normatif, namun implementasinya masih cenderung formalistik dan belum sepenuhnya terinternalisasi dalam praktik organisasi. Sebaliknya, Singapura menunjukkan pendekatan yang lebih adaptif melalui penekanan pada mekanisme kepatuhan internal, sehingga prinsip-prinsip tersebut lebih operasional dalam praktik. Hal ini menunjukkan bahwa pengaturan di Indonesia masih memiliki karakter *autonomous*, karena berfokus pada kepatuhan terhadap norma, sedangkan Singapura lebih mencerminkan hukum responsif yang menekankan efektivitas dan adaptivitas dalam implementasi. Selain itu, meskipun prinsip-prinsip dalam UU PDP telah sejalan dengan standar internasional, penerapannya belum sepenuhnya mencerminkan prinsip *accountability* dalam APEC Privacy Framework, khususnya dalam memastikan bahwa organisasi secara aktif bertanggung jawab atas pengelolaan data yang dilakukan.

Hak subjek data pribadi merupakan salah satu elemen fundamental dalam rezim pelindungan data pribadi, yang bertujuan untuk memberikan kontrol kepada individu atas data yang dimilikinya. Dalam UU PDP, hak-hak tersebut meliputi antara lain hak untuk memperoleh informasi, hak untuk mengakses data, hak untuk memperbaiki dan menghapus data, serta hak untuk menarik persetujuan atas pemrosesan data pribadi. Dalam perspektif hukum modern, pengakuan terhadap hak subjek data mencerminkan pergeseran paradigma dari pelindungan data sebagai objek menjadi pelindungan terhadap individu sebagai pemilik data. Kondisi ini menunjukkan bahwa individu tidak lagi diposisikan secara pasif, melainkan sebagai pihak yang memiliki kendali terhadap penggunaan data pribadinya. Pendekatan ini dikenal sebagai *data subject-centric approach*, yang memberikan ruang lebih besar bagi individu untuk mengontrol data mereka dalam ekosistem digital (Kuner, 2017; Zhao, 2024). Lebih lanjut, undang-undang ini juga mengakui berbagai hak penting lainnya, seperti hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi, yang sering dikaitkan dengan konsep *right to be forgotten*. Selain itu, terdapat pula hak untuk menarik kembali persetujuan atas pemrosesan data serta hak untuk mengajukan keberatan terhadap tindakan pengambilan keputusan yang didasarkan semata-mata pada pemrosesan otomatis, termasuk *profiling* (UU PDP, 2022).

Namun demikian, dalam praktiknya, pelaksanaan hak-hak tersebut masih menghadapi berbagai kendala. Beberapa penelitian menunjukkan bahwa tingkat kesadaran masyarakat terhadap hak atas data pribadi masih relatif rendah, sehingga banyak individu yang tidak sepenuhnya memahami bagaimana data mereka dikumpulkan dan digunakan (Razi et al., 2024). Selain itu, terdapat pula ketimpangan posisi antara subjek data dan pengendali data, di mana perusahaan memiliki kendali yang lebih besar dalam pengelolaan data dibandingkan individu. Dalam konteks perusahaan digital (*startup*), tantangan tersebut menjadi semakin kompleks. Pengolahan data dalam skala besar serta penggunaan teknologi otomatis dalam pengambilan keputusan membuat pemenuhan hak subjek data menjadi tidak sederhana. Misalnya, penerapan hak akses dan penghapusan data dapat menjadi sulit ketika data tersebar dalam berbagai sistem atau digunakan untuk kepentingan analitik dan pengembangan produk (Wu, 2024). Sementara itu, Singapura melalui PDPA juga mengakui hak subjek data, khususnya hak akses dan koreksi data pribadi. Namun, pengaturannya lebih menekankan pada kewajiban organisasi dalam memfasilitasi pelaksanaan hak tersebut melalui mekanisme yang praktis dan terstruktur (PDPC, 2022). Hal ini mengindikasikan bahwa, meskipun pengaturan hak subjek data dalam UU PDP telah memberikan pelindungan yang komprehensif secara normatif, efektivitasnya sangat bergantung pada

kemampuan dan komitmen perusahaan digital dalam mengimplementasikan mekanisme pemenuhan hak tersebut secara nyata.

Apabila dianalisis menggunakan Teori Perlindungan Hukum Philipus M. Hadjon, pengaturan hak subjek data dalam Undang-Undang Pelindungan Data Pribadi merupakan bentuk perlindungan hukum preventif yang bertujuan memberikan kesempatan kepada individu untuk mengendalikan penggunaan data pribadinya sebelum terjadi pelanggaran (Hadjon, 1987; Repelita, 2025). Namun, keberadaan hak secara normatif belum tentu menghasilkan perlindungan yang efektif apabila masyarakat tidak memahami hak-hak yang dimilikinya atau tidak memiliki akses yang memadai untuk menggunakan hak tersebut. Temuan ini sejalan dengan penelitian *The Awareness Gap in Personal Data Privacy* yang menunjukkan masih adanya kesenjangan pemahaman masyarakat mengenai hak atas data pribadi dalam lingkungan digital (IJSSHR, 2024). Kondisi ini menunjukkan bahwa, efektivitas perlindungan hukum tidak hanya ditentukan oleh kelengkapan norma, tetapi juga oleh tingkat literasi digital masyarakat serta kesiapan organisasi dalam menyediakan mekanisme pemenuhan hak subjek data secara mudah dan transparan.

Selain menjamin hak kepada subjek data, UU PDP juga mengatur tanggung jawab yang harus dipenuhi oleh pengendali data pribadi dalam setiap kegiatan pengolahan data. Pengaturan tersebut bertujuan untuk memastikan bahwa pemrosesan data dilakukan secara bertanggung jawab, aman, dan sesuai dengan prinsip-prinsip pelindungan data yang telah ditetapkan (UU PDP, 2022). Dalam ketentuan tersebut, pengendali data diwajibkan untuk memproses data pribadi secara terbatas, spesifik, sah, dan transparan, serta memastikan bahwa data yang diproses sesuai dengan tujuan pengumpulannya. Selain itu, pengendali data juga bertanggung jawab untuk menjaga keamanan data pribadi melalui penerapan langkah-langkah teknis dan organisasi, menjamin keakuratan data, serta menghapus data setelah masa retensi berakhir (UU PDP, 2022). Kewajiban tersebut juga didukung oleh ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mewajibkan penyelenggara sistem elektronik untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab dalam melindungi informasi elektronik dan data pengguna. Sejalan dengan itu, UU PDP tidak berdiri sendiri, melainkan membentuk rezim pelindungan data yang saling melengkapi dengan pengaturan di bidang sistem elektronik. Secara konseptual, tanggung jawab tersebut mencerminkan prinsip *accountability*, yaitu kewajiban aktif pengendali data untuk tidak hanya mematuhi ketentuan hukum, tetapi juga mampu membuktikan kepatuhan tersebut dalam praktik (Badriah et al., 2023). Namun pada kenyataannya, implementasi kewajiban tersebut masih menghadapi berbagai tantangan, terutama bagi perusahaan digital (*startup*) yang mengelola data dalam jumlah besar dan kompleks. Beberapa penelitian menunjukkan bahwa tingkat kepatuhan terhadap kewajiban pelindungan data dipengaruhi oleh kapasitas teknis, biaya kepatuhan, serta tingkat kesadaran organisasi terhadap pentingnya pelindungan data pribadi (Azza, 2024; Syailendra, 2023). Kondisi tersebut menunjukkan bahwa efektivitas pelaksanaan kewajiban pengendali data tidak hanya ditentukan oleh keberadaan norma hukum, tetapi juga oleh kesiapan organisasi dalam membangun tata kelola data yang memadai. Dengan mempertimbangkan hal tersebut, kepatuhan terhadap UU PDP memerlukan dukungan kapasitas teknis, sumber daya manusia, dan budaya kepatuhan yang berkelanjutan agar pelindungan data pribadi dapat diterapkan secara efektif dalam praktik.

Dalam konteks tersebut, pelaksanaan kewajiban pengendali data dalam praktik masih menghadapi berbagai tantangan, terutama seiring meningkatnya ancaman serangan siber yang memperbesar risiko pelanggaran keamanan data pribadi. Kondisi tersebut menunjukkan bahwa pelindungan data pribadi tidak hanya memerlukan kepatuhan terhadap ketentuan hukum, tetapi juga kesiapan teknis dan tata kelola organisasi yang memadai dalam mengelola berbagai risiko pengolahan data (Razi et al., 2024; UNCTAD, 2021). Tantangan tersebut semakin kompleks karena masih terdapat ketimpangan informasi (*information asymmetry*) antara subjek data dan pengendali data, di mana

pengguna sering kali tidak sepenuhnya memahami bagaimana data pribadi mereka dikumpulkan, diproses, dan dimanfaatkan. Persetujuan (*consent*) yang diberikan melalui *terms and conditions* juga belum tentu mencerminkan kehendak yang benar-benar sadar dan terinformasi, sehingga berpotensi mengurangi efektivitas pelindungan hak subjek data. Selain itu, risiko kebocoran data (*data breach*) akibat serangan siber maupun kesalahan teknis menunjukkan bahwa kepatuhan formal terhadap regulasi belum tentu diikuti oleh kemampuan organisasi dalam menerapkan pelindungan data secara efektif, meningkatnya ancaman serangan siber yang memperbesar risiko pelanggaran keamanan data pribadi (IBM, 2024). Sejalan dengan kondisi tersebut, efektivitas kewajiban pengendali data dalam UU PDP tidak cukup diukur dari kelengkapan pengaturannya, melainkan juga dari kemampuan organisasi membangun sistem keamanan informasi, meningkatkan kapasitas sumber daya manusia, serta menumbuhkan budaya kepatuhan yang berkelanjutan, khususnya bagi perusahaan digital (*startup*) yang mengelola data dalam jumlah besar dan lintas yurisdiksi. Sebaliknya, pendekatan Singapura memberikan ruang yang lebih besar bagi organisasi untuk menyesuaikan mekanisme kepatuhan sesuai perkembangan teknologi, yang didukung oleh tata kelola data dan keamanan siber yang lebih terintegrasi (Lim, 2021).

Jika ditinjau melalui Teori Hukum Responsif dari Nonet dan Selznick, pengaturan kewajiban pengendali data di Indonesia dan Singapura menunjukkan karakter implementasi yang berbeda (Nonet & Selznick, 1978; Pahlevi et al., 2025). Indonesia cenderung menempatkan hukum sebagai instrumen yang menekankan kepastian norma melalui pengaturan kewajiban yang rinci disertai sanksi yang tegas. Sebaliknya, Singapura tidak hanya menekankan kepatuhan terhadap norma hukum, tetapi juga mendorong organisasi untuk membangun mekanisme kepatuhan internal melalui penyusunan kebijakan pelindungan data, audit berkala, serta pengawasan aktif oleh PDPC. Perbedaan tersebut menunjukkan bahwa pendekatan Singapura lebih mencerminkan karakter hukum responsif karena mampu menyesuaikan penerapan hukum dengan kebutuhan organisasi dan perkembangan ekosistem digital yang dinamis. Bagi perusahaan digital (*startup*), pendekatan tersebut memberikan fleksibilitas yang lebih besar dalam membangun sistem kepatuhan tanpa mengurangi standar pelindungan data pribadi yang harus dipenuhi. Temuan ini menunjukkan bahwa penguatan tata kelola organisasi, pembinaan regulatif, dan mekanisme pengawasan yang berkelanjutan perlu dikembangkan sebagai pelengkap pendekatan normatif dalam UU PDP agar mampu meningkatkan efektivitas pelindungan data pribadi sekaligus merespons perkembangan teknologi digital secara lebih adaptif. Meskipun penguatan tata kelola organisasi merupakan prasyarat penting dalam pelindungan data pribadi, efektivitas regulasi pada akhirnya ditentukan oleh bagaimana mekanisme penegakan hukum dijalankan dalam praktik.

Penegakan hukum merupakan elemen yang menentukan efektivitas pelindungan data pribadi karena keberhasilan suatu regulasi tidak hanya diukur dari kelengkapan norma, tetapi juga dari konsistensi penerapannya dalam praktik. Kondisi tersebut tercermin dari masih tingginya kasus kebocoran data pribadi di Indonesia dalam beberapa tahun terakhir, baik pada sektor publik maupun perusahaan digital. Kasus kebocoran data BPJS Kesehatan, Tokopedia, dan data pemilih KPU menunjukkan bahwa pelindungan data pribadi masih menghadapi tantangan serius, khususnya dalam aspek keamanan sistem, pengawasan, dan akuntabilitas organisasi (Kementerian Komunikasi dan Informatika, 2023). Fenomena tersebut juga sejalan dengan IBM *Cost of a Data Breach Report 2024* yang menunjukkan bahwa meningkatnya kompleksitas ancaman siber menyebabkan organisasi menghadapi biaya pemulihan yang semakin besar apabila gagal menerapkan tata kelola data yang efektif (IBM, 2024). Dari perspektif APEC Privacy Framework, kasus-kasus tersebut mengindikasikan belum optimalnya penerapan prinsip *Security Safeguards* dan *Accountability*, karena organisasi belum mampu menjamin keamanan data pribadi maupun membuktikan bahwa mekanisme pelindungan data telah diterapkan secara efektif. Kondisi tersebut juga menunjukkan bahwa kepatuhan formal terhadap ketentuan UU PDP belum selalu diikuti oleh implementasi tata kelola data yang memadai. Temuan ini sejalan dengan Azza (2024), Razi et al. (2024), dan Syailendra (2023) yang menyatakan bahwa

lemahnya penegakan hukum dan rendahnya kapasitas organisasi masih menjadi faktor utama meningkatnya pelanggaran pelindungan data pribadi di Indonesia. Selain itu, perkembangan litigasi pelindungan data menunjukkan bahwa sebagian besar mekanisme penegakan hukum masih bersifat reaktif, yaitu baru berjalan setelah terjadi pelanggaran, sehingga fungsi preventif belum terlaksana secara optimal (Chui et al., 2022). Tantangan tersebut semakin kompleks karena karakter aliran data yang bersifat lintas batas menyulitkan penegakan yurisdiksi dan koordinasi antarnegara, sebagaimana dikemukakan oleh (Kuner, 2017; Zhao, 2024). Berdasarkan kondisi tersebut, efektivitas penegakan hukum pelindungan data pribadi tidak hanya bergantung pada keberadaan sanksi dalam UU PDP, tetapi juga memerlukan penguatan kelembagaan, peningkatan kapasitas pengawasan, serta kerja sama internasional agar mampu menjawab tantangan pengelolaan data dalam ekosistem digital yang semakin terintegrasi. Selain ketentuan dalam UU PDP, kewajiban penyelenggara sistem elektronik dalam menjaga keamanan sistem dan data pengguna juga diatur dalam UU ITE serta PP PSTE. Kedua regulasi tersebut memperkuat kewajiban organisasi dalam menerapkan sistem elektronik yang andal, aman, dan bertanggung jawab sebagai bagian dari upaya pencegahan kebocoran data pribadi.

Kasus kebocoran data Tokopedia memperlihatkan bahwa kepatuhan terhadap pelindungan data tidak dapat diukur hanya dari keberadaan kebijakan privasi, melainkan dari kemampuan organisasi menerapkan sistem keamanan yang mampu mengantisipasi ancaman siber secara berkelanjutan. Demikian pula, kebocoran data BPJS Kesehatan menunjukkan bahwa kewajiban pengendali data untuk menerapkan langkah-langkah teknis dan organisatoris sebagaimana diatur dalam UU PDP belum sepenuhnya diimplementasikan secara efektif. Dari perspektif APEC Privacy Framework, peristiwa tersebut mencerminkan belum optimalnya penerapan prinsip *Security Safeguards* dan *Accountability*, karena organisasi belum mampu menjamin keamanan data maupun membuktikan bahwa mekanisme pelindungan data telah diterapkan secara memadai (APEC, 2015). Sementara itu, kebocoran data pemilih KPU mengindikasikan bahwa tantangan pelindungan data juga dihadapi oleh lembaga publik, sehingga keberadaan regulasi belum secara otomatis menjamin tingkat kepatuhan organisasi. Secara yuridis, ketiga kasus tersebut menunjukkan adanya kesenjangan antara kewajiban hukum pengendali data sebagaimana diatur dalam UU PDP dengan implementasinya dalam praktik. Temuan ini sejalan dengan Azza (2024), Razi et al. (2024), Syailendra (2023), serta Kuner (2017) yang menegaskan bahwa efektivitas pelindungan data tidak hanya bergantung pada substansi hukum, tetapi juga pada kapasitas organisasi, mekanisme pengawasan, dan penerapan langkah-langkah teknis yang memadai. Hal ini mengindikasikan bahwa permasalahan utama pelindungan data pribadi di Indonesia tidak terletak pada ketiadaan regulasi, melainkan pada kesenjangan antara norma hukum (*das sollen*) dan implementasinya (*das sein*), sehingga penguatan kelembagaan, budaya kepatuhan, dan mekanisme pengawasan menjadi prasyarat utama bagi efektivitas pelindungan data pribadi. Jika dibandingkan dengan Singapura, pendekatan penegakan hukum cenderung lebih tegas dan terstruktur, dengan peran aktif otoritas pengawas dalam menjatuhkan sanksi serta memberikan panduan kepatuhan kepada organisasi. Hal ini berkontribusi pada tingkat kepatuhan yang relatif lebih tinggi di kalangan perusahaan digital (Chui et al., 2022). Melalui PDPC, penegakan hukum di Singapura dilakukan secara lebih aktif dan responsif, baik dalam penanganan pengaduan maupun dalam proses investigasi pelanggaran. Kondisi ini membuat proses pembuktian menjadi lebih efisien dan tidak sepenuhnya dibebankan kepada korban. Di samping itu, PDPA juga mengizinkan PDPC menjatuhkan denda administratif hingga S\$1 juta, atau hingga 10% dari omzet tahunan organisasi di Singapura bagi perusahaan dengan omzet diatas \$10 juta, selain itu terdapat juga sanksi pidana berupa penjara hingga tiga tahun untuk pelanggaran tertentu, yang menunjukkan adanya upaya untuk menciptakan efek jera terhadap pelaku pelanggaran data pribadi (PDPC, 2022). Atas dasar tersebut, dalam konteks Indonesia, diperlukan pendekatan yang lebih komprehensif dalam penegakan hukum, yang mencakup aspek regulasi, teknologi, serta kesadaran pelaku usaha. Dengan mempertimbangkan hal tersebut dapat disimpulkan bahwa meskipun kerangka hukum di Indonesia telah berkembang, tetapi efektivitas penegakan hukum masih memerlukan

penguatan yang signifikan, terutama dalam hal pengawasan, koordinasi, dan penerapan sanksi yang konsisten. Peningkatan kasus kebocoran data menunjukkan bahwa pelindungan data pribadi tidak hanya merupakan isu hukum, tetapi juga berkaitan erat dengan aspek teknis dan keamanan sistem informasi (IJSSHR, 2024; UNCTAD, 2021).

Hal ini mengindikasikan bahwa, dalam konteks Indonesia, diperlukan pendekatan yang lebih komprehensif dalam penegakan hukum, yang mencakup aspek regulasi, teknologi, serta kesadaran pelaku usaha. Perbandingan mekanisme penegakan hukum di Indonesia dan Singapura menunjukkan bahwa efektivitas pelindungan data pribadi tidak hanya ditentukan oleh kualitas regulasi, tetapi juga oleh kapasitas kelembagaan dan mekanisme pengawasan. Temuan tersebut menunjukkan bahwa penguatan pelindungan data pribadi tidak dapat dilakukan hanya melalui penyempurnaan hukum nasional, melainkan juga memerlukan harmonisasi standar pelindungan data yang mampu menjawab tantangan pengelolaan data lintas batas. Maka dari itu, pembahasan selanjutnya mengkaji arah harmonisasi pengaturan pelindungan data pribadi di Indonesia dan Singapura berdasarkan prinsip-prinsip dalam APEC Privacy Framework.

Pengaturan pelindungan data pribadi memiliki relevansi yang sangat signifikan terhadap operasional perusahaan digital (*startup*), mengingat model bisnis *startup* pada umumnya sangat bergantung pada pengumpulan, pengolahan, dan pemanfaatan data pribadi pengguna (OECD, 2013). Dalam era ekonomi digital, data tidak hanya berfungsi sebagai alat pendukung, tetapi telah berkembang menjadi aset strategis yang menentukan inovasi, pengembangan layanan, dan daya saing perusahaan. Pemanfaatan data dalam skala besar memungkinkan perusahaan melakukan analisis perilaku pengguna, personalisasi layanan, serta pengambilan keputusan berbasis data. Namun, praktik tersebut juga meningkatkan risiko terhadap pelindungan privasi apabila tidak diimbangi dengan mekanisme pengelolaan data yang transparan, akuntabel, dan aman, sehingga berpotensi menimbulkan berbagai bentuk pelanggaran privasi dalam ekosistem digital (Wu, 2024). Dalam konteks hukum, pengelolaan data oleh perusahaan digital juga menimbulkan implikasi lintas yurisdiksi yang kompleks, terutama dalam kegiatan transfer data antarnegara (Zhang, 2024; Zhao, 2024). Kondisi tersebut menjadi tantangan tersendiri bagi *startup* yang beroperasi secara global karena harus memenuhi berbagai standar pelindungan data yang berbeda, menanggung biaya kepatuhan yang lebih tinggi, serta membangun kapasitas teknis yang memadai agar pengelolaan data tetap sesuai dengan ketentuan hukum di setiap yurisdiksi. Sejalan dengan kondisi tersebut, harmonisasi standar pelindungan data pribadi menjadi semakin penting untuk menciptakan kepastian hukum sekaligus mendukung keberlanjutan inovasi dalam ekonomi digital.

Kebutuhan akan harmonisasi pelindungan data pribadi tidak selalu mengharuskan adanya penyamaan regulasi di setiap negara. Mengingat perbedaan sistem hukum, tingkat perkembangan ekonomi digital, dan kepentingan nasional, pendekatan yang lebih realistis adalah membangun kesesuaian prinsip melalui kerangka yang dapat diterapkan secara fleksibel. Dalam konteks tersebut, APEC Privacy Framework menjadi salah satu instrumen yang relevan karena menawarkan prinsip-prinsip pelindungan data pribadi yang dirancang untuk mendukung keseimbangan antara pelindungan hak individu dan kelancaran arus data lintas batas (APEC, 2015). Berbeda dengan pendekatan yang lebih mengikat seperti GDPR, APEC Privacy Framework mengedepankan interoperabilitas sehingga setiap negara tetap dapat mempertahankan karakteristik sistem hukumnya tanpa menghambat aktivitas ekonomi digital. Dengan mempertimbangkan hal tersebut, kerangka ini digunakan sebagai alat analisis dalam penelitian untuk menilai sejauh mana pengaturan pelindungan data pribadi di Indonesia dan Singapura telah selaras dengan prinsip-prinsip pelindungan data yang berlaku di kawasan Asia-Pasifik.

Menurut Nonet dan Selznick, hukum responsif merupakan hukum yang mampu menyesuaikan diri terhadap perubahan kebutuhan masyarakat dan perkembangan sosial, termasuk perubahan yang dipicu oleh kemajuan teknologi (Nonet & Selznick, 1978; Pahlevi et al., 2025). Dalam konteks pelindungan data pribadi, perkembangan ekonomi digital dan arus data lintas batas menuntut regulasi

yang tidak hanya memberikan kepastian hukum, tetapi juga mampu beradaptasi terhadap dinamika teknologi serta kebutuhan kerja sama antarnegara. Oleh karena itu, harmonisasi pelindungan data pribadi perlu dipahami sebagai upaya membangun sistem hukum yang adaptif melalui penyelarasan prinsip-prinsip dasar tanpa menghilangkan karakteristik sistem hukum masing-masing negara.

Meskipun Indonesia dan Singapura memiliki pendekatan regulasi yang berbeda, harmonisasi pelindungan data pribadi tidak mengharuskan kedua negara menerapkan sistem hukum yang seragam. Mengingat perbedaan tradisi hukum, kapasitas kelembagaan, serta kebutuhan ekonomi digital masing-masing negara, model harmonisasi yang lebih tepat adalah *interoperability*, yaitu kesesuaian prinsip pelindungan data tanpa menghilangkan karakteristik hukum nasional. Menurut Zhao (2024), interoperabilitas memungkinkan berbagai rezim pelindungan data saling diakui sehingga dapat mendukung kelancaran arus data lintas batas tanpa mengurangi tingkat pelindungan hak individu. Pandangan tersebut diperkuat oleh Liu (2023) yang menyatakan bahwa pembangunan mekanisme saling percaya (*mutual trust*) antarnegara menjadi prasyarat utama dalam tata kelola data lintas batas di kawasan Asia. Sejalan dengan itu, Kuner (2017) menjelaskan bahwa pendekatan interoperabilitas lebih efektif dibandingkan harmonisasi yang bersifat seragam karena memberikan fleksibilitas bagi setiap negara untuk mempertahankan karakteristik sistem hukumnya, sekaligus menciptakan standar minimum yang dapat diterapkan bersama. Temuan tersebut juga sejalan dengan Mardyansyah et al. (2025) yang menekankan bahwa harmonisasi pelindungan data pribadi sebaiknya diarahkan pada penyelarasan prinsip-prinsip fundamental tanpa menghilangkan karakteristik sistem hukum nasional. Hal ini mengindikasikan bahwa, model interoperabilitas merupakan pendekatan yang paling relevan bagi Indonesia dan Singapura dalam mewujudkan harmonisasi pelindungan data pribadi di kawasan Asia-Pasifik.

Pengaturan pelindungan data pribadi pada era ekonomi digital tidak lagi dapat dipandang sebagai persoalan domestik semata, melainkan telah berkembang menjadi isu lintas batas yang memerlukan harmonisasi antarnegara. Perkembangan perusahaan digital (*startup*) yang beroperasi melalui platform digital menyebabkan meningkatnya arus data pribadi lintas negara (*cross-border data flow*), sehingga perbedaan standar pelindungan data berpotensi menimbulkan ketidakpastian hukum bagi pelaku usaha maupun risiko terhadap hak privasi individu (Kuner, 2017; OECD, 2023; Zhang, 2024). Tantangan tersebut semakin kompleks dengan berkembangnya *big data*, *artificial intelligence*, dan analisis perilaku pengguna yang memperluas pemanfaatan data pribadi dalam kegiatan ekonomi digital. Kondisi ini tercermin dari berbagai kasus kebocoran data di Indonesia, seperti Tokopedia, BPJS Kesehatan, dan Komisi Pemilihan Umum (KPU), yang menunjukkan bahwa lemahnya pengawasan, kapasitas teknis, dan tata kelola organisasi masih menjadi hambatan dalam mewujudkan pelindungan data yang efektif. Sejalan dengan kondisi tersebut, harmonisasi pengaturan tidak hanya bertujuan menyelaraskan standar pelindungan data pribadi, tetapi juga membangun mekanisme kerja sama yang mampu mendukung keamanan data, kepastian hukum, dan kelancaran arus data lintas batas. Dalam konteks tersebut, APEC Privacy Framework menjadi landasan yang relevan karena menekankan prinsip *accountability*, *security safeguards*, dan pelindungan data lintas batas sebagai dasar bagi pengembangan kerja sama regional di kawasan Asia-Pasifik.

APEC Privacy Framework merupakan salah satu kerangka regional yang dibentuk untuk mendorong harmonisasi pelindungan data pribadi di kawasan Asia-Pasifik, khususnya dalam mendukung arus data lintas batas (*cross-border data flow*) yang aman dan bertanggung jawab. Framework ini dirancang untuk menciptakan keseimbangan antara pelindungan privasi individu dan kebutuhan pertumbuhan ekonomi digital, mengingat perkembangan teknologi telah meningkatkan pertukaran data antarnegara secara signifikan (APEC, 2015; Kuner, 2017). Dalam APEC Privacy Framework, pelindungan data pribadi tidak hanya dipahami sebagai bentuk kepatuhan hukum semata, tetapi juga sebagai bagian dari tanggung jawab organisasi dalam memastikan keamanan dan akuntabilitas pengelolaan data. Dengan mempertimbangkan hal tersebut, *framework* menekankan

sejumlah prinsip penting, seperti *preventing harm*, *notice*, *collection*, *information*, *security safeguards*, serta *accountability* (APEC, 2015). Prinsip-prinsip tersebut bertujuan untuk menciptakan standar minimum pelindungan data yang dapat diterapkan secara fleksibel oleh negara anggota tanpa harus menghilangkan karakteristik sistem hukumnya masing-masing. Pendekatan ini menunjukkan bahwa pelindungan data pribadi dalam ekonomi digital memerlukan model regulasi yang adaptif terhadap perkembangan teknologi dan aktivitas bisnis lintas negara (Lynskey, 2024).

Berbeda dengan pendekatan harmonisasi yang bersifat seragam (*uniformity*), APEC Privacy Framework lebih menekankan pada interoperabilitas antar sistem hukum nasional (Kuner, 2017; Liu, 2023; Zhao, 2024). Pendekatan ini memungkinkan setiap negara mempertahankan karakteristik sistem hukumnya masing-masing, namun tetap memiliki standar pelindungan data yang kompatibel untuk mendukung kerja sama ekonomi digital regional (Liu, 2023). Model interoperabilitas dinilai lebih relevan dalam menghadapi kompleksitas pengelolaan data pribadi pada era globalisasi digital, khususnya terkait transfer data lintas batas dan aktivitas perusahaan digital multinasional. Bagi Indonesia dan Singapura, pendekatan tersebut menjadi alternatif yang lebih realistis dibandingkan harmonisasi yang bersifat seragam karena kedua negara memiliki karakteristik sistem hukum, kapasitas kelembagaan, dan tingkat perkembangan ekonomi digital yang berbeda. Meskipun demikian, prinsip-prinsip dalam APEC Privacy Framework pada dasarnya telah mulai tercermin dalam pengaturan pelindungan data pribadi di kedua negara, terutama terkait prinsip keamanan data, persetujuan, dan akuntabilitas pengendali data. Oleh karena itu, model interoperabilitas yang ditawarkan melalui APEC Privacy Framework menjadi pendekatan yang paling relevan untuk mendukung harmonisasi pelindungan data pribadi di kawasan Asia-Pasifik tanpa menghilangkan karakteristik sistem hukum nasional masing-masing, sekaligus memperkuat kepastian hukum dan mendukung perkembangan ekonomi digital regional (Wu, 2024).

Implementasi model interoperabilitas tersebut dapat didukung melalui berbagai mekanisme kerja sama regional, salah satunya APEC Cross-Border Privacy Rules (CBPR) System yang dirancang untuk memfasilitasi transfer data pribadi lintas batas melalui pengakuan bersama terhadap standar pelindungan data di antara negara peserta. Selain itu, ASEAN Framework on Personal Data Protection juga memberikan pedoman bagi negara-negara di kawasan Asia Tenggara dalam menyelaraskan prinsip-prinsip pelindungan data pribadi tanpa mengharuskan unifikasi sistem hukum nasional. Dalam konteks Indonesia, meskipun UU PDP telah mengadopsi berbagai prinsip yang sejalan dengan APEC Privacy Framework, implementasinya masih menghadapi tantangan, terutama pada aspek kelembagaan, pengawasan, dan efektivitas penegakan hukum (Razi et al., 2024; Syailendra, 2023). Salah satu bentuk penguatan tersebut berkaitan dengan amanat Pasal 58 ayat (3) UU PDP mengenai pembentukan lembaga pelindungan data pribadi yang bertanggung jawab kepada Presiden. Berdasarkan Pasal 59 dan Pasal 60 UU PDP, lembaga tersebut memiliki tugas untuk merumuskan kebijakan dan strategi pelindungan data pribadi, mengawasi kepatuhan pengendali dan prosesor data pribadi, menjatuhkan sanksi administratif, serta memfasilitasi penyelesaian sengketa di luar pengadilan (UU PDP, 2022). Penguatan kelembagaan tersebut sejalan dengan prinsip *accountability* dalam APEC Privacy Framework yang menekankan pentingnya mekanisme pengawasan dan tanggung jawab organisasi dalam pengelolaan data pribadi. Oleh karena itu, pembentukan lembaga pelindungan data pribadi yang independen, disertai penguatan mekanisme kepatuhan organisasi dan kerja sama regional, menjadi langkah strategis dalam mendukung harmonisasi pelindungan data pribadi di Indonesia sekaligus meningkatkan efektivitas implementasi UU PDP. Secara normatif, pengaturan pelindungan data pribadi di Indonesia tidak hanya bersumber dari UU PDP, tetapi juga didukung oleh UU ITE dan PP PSTE yang mengatur penyelenggaraan sistem elektronik sebagai sarana pemrosesan data pribadi. Integrasi ketiga regulasi tersebut menunjukkan bahwa arah harmonisasi tidak hanya memerlukan penyelarasan substansi hukum, tetapi juga penguatan implementasi dalam tata kelola sistem elektronik.

Berdasarkan hasil perbandingan tersebut, Indonesia dan Singapura pada dasarnya telah mengadopsi prinsip-prinsip pelindungan data pribadi yang sejalan dengan APEC Privacy Framework, termasuk prinsip *consent*, *accountability*, *security safeguards*, dan pembatasan tujuan pengolahan data (UU PDP, 2022). Perbedaan utama antara kedua negara tidak terletak pada substansi pengaturannya, melainkan pada efektivitas implementasi, kapasitas kelembagaan, serta mekanisme pengawasan yang mendukung kepatuhan organisasi. Indonesia masih menghadapi berbagai tantangan dalam aspek pengawasan, penegakan hukum, dan tata kelola organisasi sehingga penerapan prinsip *accountability* belum sepenuhnya berjalan secara efektif dalam praktik (Custers et al., 2022; Lynskey, 2024; Razi et al., 2024; Syailendra, 2023). Sebaliknya, Singapura menunjukkan implementasi yang lebih operasional melalui pengawasan aktif oleh PDPC yang mendorong organisasi tidak hanya mematuhi ketentuan hukum, tetapi juga mampu membuktikan kepatuhan tersebut melalui mekanisme internal yang terstruktur (Badriah et al., 2023; PDPC, 2022). Temuan ini menunjukkan bahwa efektivitas pelindungan data pribadi tidak hanya ditentukan oleh kelengkapan regulasi, tetapi juga oleh kemampuan sistem hukum dalam mengintegrasikan pengawasan, kepatuhan organisasi, dan kapasitas kelembagaan secara berkelanjutan. Berdasarkan kondisi tersebut, dalam perspektif Teori Hukum Responsif, pendekatan Singapura lebih mencerminkan hukum yang adaptif terhadap perkembangan ekonomi digital, sedangkan Indonesia masih berada pada tahap penguatan implementasi agar prinsip-prinsip APEC Privacy Framework dapat diterapkan secara lebih efektif dalam praktik.

Berdasarkan hasil analisis komparatif, model harmonisasi yang paling relevan untuk diterapkan antara Indonesia dan Singapura bukanlah model unifikasi hukum, melainkan model interoperabilitas sebagaimana dikembangkan dalam APEC Privacy Framework. Pendekatan tersebut juga sejalan dengan perkembangan kajian harmonisasi pelindungan data pribadi yang menekankan pentingnya penyelarasan prinsip-prinsip dasar tanpa menghilangkan karakteristik sistem hukum nasional masing-masing negara (Mardyansyah et al., 2025). Model ini memungkinkan masing-masing negara mempertahankan karakteristik sistem hukumnya, namun tetap memiliki standar pelindungan data pribadi yang kompatibel dalam mendukung arus data lintas batas (*cross-border data flow*) (Liu, 2023). Dalam konteks tersebut, harmonisasi diarahkan pada penyelarasan prinsip-prinsip utama seperti *accountability*, *security safeguards*, dan *cross-border privacy protection* tanpa mengharuskan kesamaan bentuk regulasi secara mutlak. Pendekatan ini dinilai lebih realistis mengingat adanya perbedaan sistem hukum, tingkat kesiapan kelembagaan, dan kapasitas pengawasan antara Indonesia dan Singapura. Kondisi ini menunjukkan bahwa, interoperabilitas dapat menjadi model harmonisasi yang mendukung kepastian hukum sekaligus fleksibilitas dalam perkembangan ekonomi digital regional. Mekanisme tersebut juga dapat diintegrasikan dengan skema kerja sama regional seperti APEC Cross-Border Privacy Rules (CBPR) System dan ASEAN Framework on Personal Data Protection untuk memperkuat interoperabilitas pelindungan data lintas batas. Harmonisasi tersebut dapat diimplementasikan melalui beberapa mekanisme. Pertama, pembentukan lembaga pelindungan data pribadi yang independen sebagaimana diamanatkan dalam UU PDP. Kedua, penguatan mekanisme kepatuhan organisasi melalui kewajiban audit pelindungan data, penunjukan petugas pelindungan data (*data protection officer*), dan pelaporan insiden kebocoran data secara berkala. Ketiga, peningkatan kerja sama regional dalam pengawasan transfer data lintas batas melalui pengembangan standar teknis yang mengacu pada prinsip-prinsip APEC Privacy Framework. Dengan adanya mekanisme tersebut, harmonisasi tidak hanya berhenti pada tingkat normatif, tetapi juga dapat diterapkan secara operasional dalam praktik. Dari perspektif pengembangan hukum (*ius constituendum*), *roadmap* harmonisasi pelindungan data pribadi di Indonesia dapat dilakukan melalui tiga tahapan. Tahap pertama adalah penguatan kelembagaan melalui pembentukan otoritas pelindungan data pribadi yang independen dan penyusunan regulasi pelaksana yang masih diperlukan. Tahap kedua adalah penguatan kepatuhan organisasi melalui penerapan standar keamanan data, audit kepatuhan, dan peningkatan literasi pelindungan data bagi pelaku usaha digital. Tahap ketiga adalah integrasi yang lebih luas dengan

kerangka kerja regional melalui peningkatan kerja sama transfer data lintas batas dan pengembangan mekanisme interoperabilitas yang selaras dengan APEC Privacy Framework. Melalui tahapan tersebut, harmonisasi pelindungan data pribadi tidak hanya berfungsi sebagai instrumen regulasi, tetapi juga sebagai sarana untuk meningkatkan kepercayaan dalam ekonomi digital kawasan Asia-Pasifik. Arah harmonisasi pengaturan pelindungan data pribadi di Indonesia dan Singapura pada dasarnya perlu diarahkan pada penguatan efektivitas implementasi hukum dalam menghadapi perkembangan ekonomi digital dan arus data lintas batas (*cross-border data flow*). Dalam konteks APEC Privacy Framework, harmonisasi tidak dimaknai sebagai penyamaan sistem hukum secara mutlak, melainkan sebagai upaya untuk menciptakan standar pelindungan data yang interoperabel dan mampu mendukung kerja sama ekonomi digital regional (APEC, 2015; OECD, 2023). Perkembangan terbaru menunjukkan bahwa harmonisasi pelindungan data pribadi tidak lagi hanya berfokus pada penyamaan prinsip-prinsip hukum, tetapi juga pada pembangunan interoperabilitas antar rezim pelindungan data. OECD menegaskan bahwa tantangan utama saat ini terletak pada kemampuan setiap negara untuk menciptakan mekanisme yang memungkinkan transfer data lintas batas berlangsung secara aman tanpa mengurangi tingkat pelindungan hak individu. Oleh karena itu, interoperabilitas menjadi pendekatan yang semakin relevan dalam mendukung ekonomi digital global (OECD, 2023). Dalam konteks Indonesia, penguatan harmonisasi perlu difokuskan pada aspek implementasi dan pengawasan terhadap pelaksanaan Undang-Undang Pelindungan Data Pribadi. Meskipun secara normatif UU PDP telah mengadopsi berbagai prinsip yang sejalan dengan APEC Privacy Framework, efektivitasnya masih menghadapi berbagai tantangan, terutama terkait belum optimalnya pengawasan, mekanisme kepatuhan organisasi, serta penerapan sanksi yang konsisten. Dengan mempertimbangkan hal tersebut, diperlukan penguatan lembaga pengawas yang independen dan responsif agar penegakan hukum pelindungan data pribadi dapat berjalan secara lebih efektif.

Selain itu, harmonisasi juga perlu diarahkan pada penguatan prinsip *accountability* dalam praktik pengelolaan data pribadi oleh perusahaan digital (*startup*). Dalam hal ini, pendekatan Singapura melalui PDPA dapat menjadi salah satu acuan, khususnya dalam penerapan mekanisme kepatuhan internal, pengawasan aktif oleh otoritas, serta kewajiban organisasi untuk mampu membuktikan kepatuhan terhadap pengelolaan data pribadi. Pendekatan tersebut menunjukkan bahwa efektivitas pelindungan data tidak hanya bergantung pada keberadaan norma hukum, tetapi juga pada kemampuan organisasi dalam mengimplementasikan standar pelindungan data secara operasional. Di samping itu, diperlukan pula pengembangan pedoman teknis dan regulasi turunan yang lebih adaptif terhadap perkembangan teknologi digital, termasuk dalam penggunaan *big data*, *artificial intelligence*, dan sistem pemrosesan data otomatis. Penguatan kerja sama regional dalam pengawasan dan transfer data lintas batas juga menjadi penting untuk mendukung interoperabilitas sistem pelindungan data pribadi antarnegara sebagaimana ditekankan dalam APEC Privacy Framework (ASEAN Privacy Regulation, 2023). Perkembangan terbaru menunjukkan bahwa mekanisme APEC Cross-Border Privacy Rules (CBPR) telah berkembang menjadi Global CBPR Forum, yang memperluas kerja sama lintas yurisdiksi serta memperkuat interoperabilitas sistem pelindungan data di tingkat internasional (IAPP, 2024). Berdasarkan hasil analisis, pendekatan Singapura lebih mencerminkan karakter hukum responsif karena regulasinya tidak hanya menetapkan kewajiban normatif, tetapi juga didukung oleh mekanisme implementasi yang adaptif melalui PDPC, *accountability*, dan pembaruan kebijakan sesuai perkembangan teknologi. Sebaliknya, Indonesia telah memiliki landasan normatif yang memadai melalui UU PDP, namun masih memerlukan penguatan implementasi agar mampu merespons dinamika ekonomi digital secara lebih efektif. Dengan demikian, arah harmonisasi pengaturan pelindungan data pribadi di Indonesia tidak hanya memerlukan penyesuaian substansi regulasi, tetapi juga penguatan aspek implementasi, pengawasan, dan kesiapan teknis dalam menghadapi perkembangan ekonomi digital. Harmonisasi tersebut diharapkan dapat menciptakan sistem pelindungan data pribadi yang lebih responsif, adaptif, dan mampu memberikan kepastian hukum bagi masyarakat maupun perusahaan digital di kawasan regional.

Simpulan

Penelitian ini menunjukkan bahwa pengaturan pelindungan data pribadi di Indonesia dan Singapura secara normatif telah mengadopsi prinsip-prinsip utama *APEC Privacy Framework*, namun

efektivitas implementasinya berbeda, terutama pada aspek kelembagaan, pengawasan, dan penegakan hukum. Dibandingkan Indonesia, Singapura memiliki sistem yang lebih operasional melalui dukungan lembaga pengawas yang kuat sehingga mampu mendorong kepatuhan organisasi secara lebih efektif. Temuan penelitian menegaskan bahwa model harmonisasi yang paling relevan adalah interoperabilitas, bukan unifikasi hukum, karena memungkinkan setiap negara mempertahankan karakteristik sistem hukumnya sekaligus mendukung kompatibilitas pelindungan data dalam arus data lintas batas. Oleh karena itu, Indonesia perlu memperkuat kelembagaan pengawas, menyempurnakan regulasi pelaksana, meningkatkan kapasitas organisasi, serta mengembangkan integrasi dengan mekanisme regional seperti *APEC Cross-Border Privacy Rules (CBPR) System* untuk mewujudkan tata kelola pelindungan data pribadi yang lebih efektif. Meskipun demikian, penelitian ini masih terbatas pada pendekatan normatif, sehingga penelitian selanjutnya disarankan mengembangkan kajian empiris mengenai implementasi regulasi dan tingkat kepatuhan organisasi, serta memperluas perbandingan dengan negara-negara ASEAN lainnya.

Referensi

- APEC. (2015). *APEC privacy framework*. [https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-\(2015\)/217_ecsg_2015-apec-privacy-framework.pdf](https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf)
- ASEAN Privacy Regulation. (2023). *Cross-border data privacy regulation in ASEAN*. <https://searchlib.utcc.ac.th/library/online/thesis/309645.pdf>
- Azmi, F., & Sanjaya, D. (2023). The importance of Personal Data Protection Act for the protection of digital society in Indonesia. *Law and Humanities Quarterly Reviews*, 2(3), 128–141. <https://doi.org/10.31014/aior.1996.02.03.77>
- Azza, V. M. (2024). Application of personal data protection on electronic signatures in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(5). <https://doi.org/10.59141/jist.v5i5.1102>
- Badriah, L., Indiahono, D., & Sukarso. (2024). Accountability in personal data protection policy in Indonesia: Learning from South Korea and Singapore. *Jurnal Bina Praja*, 16(2), 89–102. <https://doi.org/10.21787/mp.8.2.2024.89-102>
- Chui, L., Lye, A., & Lim, J. (2022). *Developments in data privacy litigation*. <https://www.twobirds.com/-/media/new-website-content/insights/pdfs/2022-personal-data-protection-digest-extract.pdf>
- Custers, B., Sears, A. M., Dechesne, F., & Georgieva, I. (2022). EU personal data protection in policy and practice. *Computer Law & Security Review*, 46, Article 105716. <https://doi.org/10.1016/j.clsr.2022.105716>
- Disemadi, H. S. (2022). Lenses of legal research: A descriptive essay on legal research methodologies. *Journal of Judicial Review*, 24(2), 289–304. <https://doi.org/10.37253/jjr.v24i2.7280>
- Google, Temasek, & Bain & Company. (2022). *e-Conomy SEA 2022 report*. https://services.google.com/fh/files/misc/e_economy_sea_2022_report.pdf
- Google, Temasek, & Bain & Company. (2024). *e-Conomy SEA 2024 report*. <https://economysea.withgoogle.com/>
- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat Indonesia*. PT Bina Ilmu.
- Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, 162, Article 113777. <https://doi.org/10.1016/j.jbusres.2023.113777>
- International Association of Privacy Professionals. (2024). *Unlocking global data privacy interoperability with CBPRs*. <https://iapp.org/news/a/unlocking-global-data-privacy-interoperability-with-cbprs/>
- IBM. (2024). *Cost of a data breach report 2024*. <https://www.ibm.com/reports/data-breach>
- International Journal of Social Science and Human Research. (2024). The awareness gap in personal data privacy: A human rights perspective. *International Journal of Social Science and Human Research*, 7(7). <https://doi.org/10.47191/ijsshr/v7-i07-84>

- Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(1), 20–29. <https://doi.org/10.58812/eslhr.v3i01.351>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Kominfo catat 94 kasus kebocoran data pribadi sejak 2019 hingga Juni 2023*. <https://nasional.kontan.co.id/news/kominfo-catat-94-kasus-kebocoran-data-pribadi-sejak-2019-hingga-juni-2023>
- Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>
- Lim, S. (2021). Cybersecurity and data protection—Singapore. *Asian Journal of Law and Society*. <https://doi.org/10.1017/als.2024.31>
- Liu, X. (2024). The dilemma of cross-border data flow and the construction of mutual trust platform in Asia. *Asian Journal of Law and Society*, 11, 488–506. <https://doi.org/10.1017/als.2024.31>
- Lynskey, O. (2024). How might the GDPR evolve? A question of politics, pace and punishment. *Computer Law & Security Review*, 54, Article 106033. <https://doi.org/10.1016/j.clsr.2024.106033>
- Mardiansyah, D. N., Sukarmi, Kusumaningrum, A., & Widyanti, Y. E. (2025). Harmonization of personal data protection principles with international standards. *Yuridika*. <https://doi.org/10.20473/ydk.v40i3.74179>
- Nonet, P., & Selznick, P. (1978). *Law and society in transition: Toward responsive law*. Harper & Row.
- Organisation for Economic Co-operation and Development. (2013). *The OECD privacy framework*. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2023). *Report on the implementation of the OECD privacy guidelines* (OECD Digital Economy Papers No. 361). OECD Publishing. <https://doi.org/10.1787/cf87ae8f-en>
- Pahlevi, A. N., Permatasari, N., & Kania, D. (2025). Comparison of the application of responsive legal theory in responding to social change in the criminal law and civil law. *Bengkoelen Justice: Jurnal Ilmu Hukum*, 15(1). https://doi.org/10.33369/j_bengkoelenjust.v15i1.40023
- Personal Data Protection Commission. (2022). *Personal data protection digest 2022*. <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/PDP-Digest-Files/2022-Personal-Data-Protection-Digest.pdf>
- Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(12), 6559–6565. <https://doi.org/10.59141/jist.v5i12.1285>
- Repelita, T. (2025). Perlindungan hukum bagi konsumen terhadap privasi data pribadi dalam era artificial intelligence di Indonesia. *Jurnal Yuridis*, 12(1), 168–180. <https://doi.org/10.35586/jjur.v12i1.12080>
- Riyadi, G. (2021). *Data privacy in the Indonesian Personal Data Protection Bill*. <https://doi.org/10.35497/341482>
- Rosadi, S. D. (2018). Protecting privacy on personal data in the digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal*, 5(1), 143–157. <https://doi.org/10.21776/ub.blj.2018.005.01.09>
- Suleiman, A. (2022). *Co-regulation in protecting personal data*. <https://doi.org/10.35497/555905>
- Syailendra, M. R. (2023). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, 14(2), Article 4. <https://doi.org/10.15742/ilrev.v14n2.4>
- Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463–2478. <https://doi.org/10.31604/jips.v8i8.2021.2463-2478>
- United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development*. https://unctad.org/system/files/official-document/der2021_en.pdf
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>
- Wu, C. (2024). Data privacy: From transparency to fairness. *Technology in Society*, 76, Article 102457. <https://doi.org/10.1016/j.techsoc.2024.102457>

- Zhang, Z. (2024). Cross-border data flow governance. *Highlights in Business, Economics and Management*. <https://doi.org/10.54097/49setj81>
- Zhao, Z. (2024). The dilemma of cross-border data flow and the construction of mutual trust platform in Asia. *Asian Journal of Law and Society*, 11(S4), 488–506. <https://doi.org/10.1017/als.2024.31>