

Perlindungan Hukum Data Pribadi Dalam Ekosistem Digital Indonesia: Analisis Implementasi Undang-Undang Nomor 27 Tahun 2022

Miranti Zafitri Oktaviani¹

¹ Universitas Pamulang, Indonesia

Korespondensi: mirantizafitri2006@email.com

Informasi Artikel

Riwayat artikel:

Received Aug 25th, 2026

Revised Sept 20th, 2026

Accepted Sept 27th, 2026

Keyword:

Personal Data Protection; Privacy Rights; PDP Law; Data Governance; Cybersecurity; Digital Economy.

ABSTRAK

Penelitian ini menganalisis perlindungan hukum data pribadi dalam ekosistem digital Indonesia setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Permasalahan penelitian berfokus pada kecukupan kerangka hak subjek data, kewajiban pengendali dan prosesor data, mekanisme pertanggungjawaban, serta tantangan implementasi pada layanan digital. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan terbatas dengan General Data Protection Regulation. Hasil penelitian menunjukkan bahwa Undang-Undang Pelindungan Data Pribadi telah membentuk kerangka hak dan kewajiban yang lebih terintegrasi dibandingkan pengaturan sektoral sebelumnya. Namun, efektivitas perlindungan tetap bergantung pada kejelasan aturan pelaksana, kapasitas kelembagaan pengawas, kesiapan pengendali dan prosesor data, serta mekanisme penanganan insiden dan pengaduan. Kajian juga menunjukkan pentingnya prinsip pembatasan tujuan, minimisasi data, keamanan, transparansi, dan akuntabilitas sebagai jembatan antara norma hukum dan praktik tata kelola data. Penelitian menyimpulkan bahwa penguatan implementasi harus diarahkan pada kepastian prosedural, pengawasan berbasis risiko, dan peningkatan kemampuan teknis maupun hukum para pemangku kepentingan.



© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

PENDAHULUAN

Transformasi digital telah mengubah cara masyarakat berinteraksi, bertransaksi, memperoleh layanan publik, dan mengelola identitas. Aktivitas tersebut menghasilkan jejak data yang semakin beragam, mulai dari identitas dasar, informasi kontak, data transaksi, lokasi, hingga data biometrik. Dalam konteks hukum, perubahan tersebut membuat hubungan antara individu dan organisasi tidak lagi hanya menyangkut kepemilikan informasi, tetapi juga menyangkut siapa yang menentukan tujuan pemrosesan, bagaimana data digunakan, berapa lama data disimpan, dan apa yang harus dilakukan ketika terjadi pelanggaran keamanan. Undang-Undang Nomor 27 Tahun 2022 menempatkan perlindungan data pribadi sebagai bagian dari perlindungan diri pribadi dan memberikan landasan hukum yang lebih terintegrasi bagi pemrosesan data di Indonesia (Republik Indonesia, 2022).

Perkembangan tersebut memiliki konsekuensi terhadap hukum privasi. Hak privasi tidak berhenti pada larangan membuka informasi secara sembarangan, tetapi mencakup kemampuan subjek data untuk mengetahui dan mengendalikan penggunaan data yang berkaitan dengannya. Fauzy dan Shandy (2023) menghubungkan UU PDP dengan hak atas privasi yang berakar pada Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Perspektif hak asasi juga terlihat dalam perkembangan hukum internasional yang terus menempatkan privasi sebagai hak yang harus dilindungi dalam lingkungan digital (Human Rights Council, 2023).

Masalah hukum muncul karena pemrosesan data berlangsung melalui rantai aktor yang panjang. Sebuah layanan digital dapat memperoleh data langsung dari pengguna, mengirimkannya

kepada penyedia infrastruktur, menggunakan analitik pihak ketiga, dan menyimpan sebagian data di luar negeri. Dalam kondisi demikian, subjek data membutuhkan aturan yang jelas mengenai tanggung jawab masing-masing pihak. Syailendra et al. (2024) menunjukkan bahwa penerbitan UU PDP merupakan perkembangan penting, tetapi implementasinya menghadapi tantangan regulasi, kelembagaan, dan teknis. Firdaus (2024) secara khusus menyoroti kebutuhan akan kepastian hukum bagi pengendali data pribadi agar kewajiban perlindungan dapat diterapkan secara terukur.

Penelitian ini bertujuan menganalisis bagaimana UU PDP membangun perlindungan hukum terhadap subjek data, bagaimana prinsip dan hak subjek data diterjemahkan menjadi kewajiban pengendali serta prosesor, dan tantangan apa yang perlu diperhatikan dalam implementasinya. Kajian juga membandingkan secara terbatas beberapa konsep dengan GDPR untuk mengidentifikasi area yang memiliki kemiripan maupun perbedaan tanpa menganggap bahwa model asing dapat dipindahkan secara langsung ke sistem hukum Indonesia.

Orisinalitas artikel terletak pada penggabungan tiga sudut pandang, yaitu perlindungan hak subjek data, kepastian tanggung jawab pelaku pemrosesan, dan kebutuhan tata kelola implementasi. Kajian sebelumnya telah membahas privasi, transaksi daring, *Electronic Know Your Customer* (e-KYC), transfer data, dan kelembagaan pengawasan secara terpisah. Artikel ini menghubungkan tema-tema tersebut dalam satu kerangka untuk melihat hubungan antara hak, kewajiban, dan penegakan hukum.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif. Metode tersebut dipilih karena objek kajian utama berupa norma hukum yang mengatur perlindungan data pribadi, hubungan hukum antara subjek data dengan pengendali atau prosesor, serta mekanisme pertanggungjawaban atas pemrosesan data. Penelitian tidak menggunakan survei lapangan atau eksperimen, melainkan menelaah bahan hukum primer dan sekunder yang relevan.

Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Nomor 27 Tahun 2022, ketentuan konstitusional mengenai perlindungan diri pribadi, serta regulasi yang berhubungan dengan aktivitas elektronik dan transaksi digital. Pendekatan konseptual digunakan untuk memahami prinsip privasi, akuntabilitas, keamanan, transparansi, pembatasan tujuan, dan minimisasi data. Pendekatan perbandingan terbatas digunakan dengan melihat *General Data Protection Regulation* (GDPR) sebagai salah satu rezim perlindungan data yang memiliki konsep hak subjek data dan kewajiban pengendali yang berkembang secara komprehensif (European Parliament & Council of the European Union, 2016).

Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta regulasi terkait sistem elektronik. Bahan hukum sekunder diperoleh dari artikel jurnal ilmiah terutama dalam rentang sepuluh tahun terakhir, termasuk penelitian mengenai hak privasi, keamanan data, *Electronic Know Your Customer* (e-KYC), transfer data, kepastian hukum pengendali, dan tata kelola perlindungan data.

Analisis dilakukan secara kualitatif dengan teknik interpretasi hukum dan analisis isi. Setiap norma diidentifikasi berdasarkan subjek yang diatur, kewajiban atau hak yang ditimbulkan, serta konsekuensi hukumnya. Selanjutnya, norma tersebut dibandingkan dengan temuan penelitian terdahulu untuk melihat kesesuaian, perbedaan, dan ruang yang masih memerlukan penguatan.

Keandalan analisis dijaga melalui penggunaan sumber hukum resmi dan publikasi ilmiah yang dapat ditelusuri. UU PDP digunakan sebagai sumber utama untuk menjelaskan definisi, prinsip, hak, kewajiban, dan sanksi, sedangkan artikel jurnal digunakan untuk membaca persoalan implementasi dan perdebatan akademik.

HASIL DAN PEMBAHASAN

A. Konfigurasi Perlindungan Data Pribadi dalam UU Nomor 27 Tahun 2022

UU PDP menghadirkan satu kerangka umum yang berlaku terhadap rangkaian pemrosesan data. Undang-undang mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung. Pengaturan tersebut penting karena identifikasi tidak selalu bergantung pada satu informasi tunggal; kombinasi beberapa informasi juga dapat membuat seseorang dapat dikenali (Republik Indonesia, 2022).

Kerangka tersebut menempatkan pemrosesan sebagai kegiatan hukum yang harus memiliki dasar dan tujuan. Prinsip pemrosesan mengharuskan pengumpulan dilakukan secara terbatas dan spesifik, sah secara hukum, serta transparan. Pemrosesan juga harus sesuai dengan tujuan, menjamin hak subjek data, menjaga akurasi, melindungi keamanan, dan mengatur penghapusan atau pemusnahan setelah masa retensi berakhir.

Tabel 1 Ringkasan Kerangka Normatif Pelindungan Data Pribadi

Aspek	Pokok Pengaturan	Implikasi Praktis
Subjek Data	Hak atas informasi, akses, koreksi, penghapusan, portabilitas, dan hak lain sesuai UU PDP	Organisasi harus menyediakan prosedur yang dapat digunakan dan diverifikasi.
Pengendali	Menentukan tujuan dan melakukan kendali pemrosesan	Perlu dasar pemrosesan, dokumentasi, dan akuntabilitas.
Prosesor	Memproses data atas nama pengendali	Tanggung jawab perlu dituangkan secara jelas dalam hubungan kontraktual dan teknis.
Keamanan	Menjaga data dari pemrosesan yang tidak sah atau insiden	Memerlukan kontrol akses, autentikasi, pencatatan, dan respons insiden.

Internasional yang menempatkan transparansi, pembatasan tujuan, dan akuntabilitas sebagai elemen penting. *General Data Protection Regulation* (GDPR) mengatur perlindungan orang perseorangan dalam pemrosesan data dan memberikan kerangka hak individu serta pengawasan yang terstruktur (European Parliament & Council of the European Union, 2016). Suari dan Sarjana (2023) menunjukkan bahwa sebelum lahirnya UU PDP, perlindungan data di Indonesia tersebar dalam berbagai peraturan sektoral. Kehadiran UU PDP memberikan kerangka yang lebih terintegrasi, tetapi efektivitasnya tetap bergantung pada konsistensi antara undang-undang, peraturan pelaksana, dan praktik organisasi. Konfigurasi tersebut memperlihatkan pergeseran dari pendekatan perlindungan yang bersifat sektoral menuju pendekatan berbasis siklus hidup data. Konsekuensinya, organisasi perlu memahami data sejak tahap pengumpulan hingga penghapusan, bukan hanya ketika data sudah digunakan atau terjadi sengketa.

B. Hak Subjek Data sebagai Pusat Perlindungan

Perlindungan hukum menjadi bermakna apabila subjek data mempunyai posisi yang cukup kuat untuk mengetahui dan mengendalikan pemrosesan datanya. UU PDP memberikan hak memperoleh informasi mengenai pemrosesan, memperbarui dan memperbaiki data, mengakses salinan data, mengakhiri pemrosesan dalam kondisi tertentu, serta hak atas penghapusan atau pemusnahan sesuai ketentuan. Hak atas informasi memiliki fungsi penting dalam memastikan transparansi. Tanpa informasi yang memadai, persetujuan atau dasar pemrosesan dapat kehilangan makna substantif karena individu tidak mengetahui data apa yang dikumpulkan, untuk tujuan apa, dan kepada siapa data dapat diteruskan. Konsep hak subjek data juga berkaitan dengan akurasi dan kualitas data. Data yang tidak akurat dapat menghasilkan konsekuensi hukum maupun ekonomi, misalnya ketika digunakan dalam verifikasi identitas atau pengambilan keputusan otomatis. Supeno et al. (2025) menekankan bahwa perlindungan data perlu dipahami melalui teori dan prinsip hukum, termasuk penghormatan terhadap hak privasi sebagai hak yang melekat pada individu. Hak atas portabilitas menunjukkan dimensi lain dari kontrol individu. Wiwoho et al. (2024) menjelaskan bahwa UU PDP telah mengenal hak portabilitas data, tetapi penerapannya membutuhkan standar teknis, arsitektur interoperabilitas, dan kompatibilitas yang jelas.

Dengan demikian, perlindungan subjek data tidak cukup diukur dari jumlah hak yang dicantumkan dalam undang-undang. Ukuran yang lebih relevan adalah apakah tersedia prosedur yang mudah digunakan, tenggat yang jelas, pihak yang bertanggung jawab, serta mekanisme penyelesaian ketika permintaan subjek data tidak dipenuhi.

C. Kewajiban Pengendali dan Prosesor Data

UU PDP membedakan pengendali data pribadi dan prosesor data pribadi. Pengendali menentukan tujuan dan melakukan kendali pemrosesan, sedangkan prosesor melakukan pemrosesan

atas nama pengendali. Perbedaan tersebut penting karena rantai pemrosesan digital sering melibatkan penyedia cloud, perusahaan analitik, penyedia pembayaran, penyedia autentikasi, dan pihak lain. Pembagian peran tersebut mengandung konsekuensi terhadap akuntabilitas. Pengendali perlu mengetahui seluruh alur pemrosesan yang berada di bawah kendalinya, termasuk penggunaan prosesor. Firdaus (2024) menunjukkan bahwa kepastian mengenai tanggung jawab pengendali menjadi penting karena ketidakjelasan norma dapat menimbulkan ketidakpastian dalam praktik.

Akuntabilitas juga berhubungan dengan keamanan. Keamanan mencakup pembatasan akses, autentikasi, pencatatan aktivitas, pemulihan, pengujian, dan respons terhadap insiden. Fitriyanti et al. (2024), dalam konteks *Electronic Know Your Customer* (e-KYC), menunjukkan pentingnya keamanan karena proses identifikasi dapat melibatkan data biometrik dan informasi sensitif. Data biometrik memperlihatkan mengapa prinsip minimisasi dan keamanan perlu diterapkan sejak awal. Apabila sebuah layanan hanya membutuhkan verifikasi tertentu, organisasi perlu menilai apakah seluruh data yang tersedia benar-benar diperlukan.

Pada transaksi pinjaman daring, persoalan menjadi lebih kompleks karena data nasabah dapat digunakan untuk penilaian kredit, komunikasi penagihan, dan kegiatan lain. Dewi dan Sulistyawan (2024) membahas perlindungan data pribadi nasabah dalam transaksi pinjaman daring dan menunjukkan pentingnya penerapan kerangka hukum perlindungan data pada hubungan digital.

D. Insiden Keamanan, Kebocoran Data, dan Pertanggungjawaban

Perlindungan data diuji secara nyata ketika terjadi kegagalan keamanan. Hukum perlu menjawab apa yang harus dilakukan untuk membatasi dampak, memberi tahu pihak yang terdampak, memulihkan sistem, dan mencegah pengulangan. Pendekatan respons insiden menempatkan kewajiban organisasi dalam perspektif pencegahan, deteksi, penanganan, dan pemulihan. Peristiwa serangan terhadap Pusat Data Nasional pada Juni 2024 menjadi salah satu contoh yang banyak dibahas dalam literatur mengenai tata kelola keamanan data di Indonesia. Yusliwidaka et al. (2024) mengaitkan peristiwa tersebut dengan pertanyaan mengenai tanggung jawab negara, tata kelola keamanan siber, dan kepatuhan terhadap kerangka hukum domestik maupun internasional.

Dalam kerangka UU PDP, kewajiban menjaga keamanan data berkaitan dengan prinsip perlindungan dan akuntabilitas. Pengamanan seharusnya menjadi bagian dari desain sistem, bukan tindakan tambahan setelah sistem beroperasi. Pendekatan ini sejalan dengan gagasan *privacy by design* dan *privacy by default* dalam diskursus perlindungan data internasional (Human Rights Council, 2024). Pertanggungjawaban membutuhkan dokumentasi. Organisasi perlu dapat menunjukkan dasar pemrosesan, tujuan, kategori data, pihak yang menerima data, masa retensi, serta langkah keamanan yang diterapkan. Dokumentasi berfungsi sebagai instrumen manajemen internal dan bukti penerapan akuntabilitas.

Dari perspektif subjek data, pemberitahuan insiden harus menghasilkan informasi yang berguna. Pemberitahuan yang hanya menyebut bahwa terjadi gangguan tanpa menjelaskan jenis data yang mungkin terdampak dan tindakan yang harus dilakukan pengguna tidak sepenuhnya membantu pemulihan risiko.

E. Transfer Data dan Interoperabilitas

Ekosistem digital membuat data dapat berpindah lintas organisasi dan lintas negara. *E-commerce*, layanan cloud, pembayaran digital, dan aplikasi berbasis platform sering menggunakan infrastruktur yang tersebar. Oleh karena itu, aturan transfer data perlu menjaga arus data sekaligus perlindungan hak subjek data.

Marischa dan Setianingrum (2024) membahas transfer data oleh perusahaan *e-commerce* dari perspektif hukum perlindungan data Indonesia. Transfer data bukan sekadar aktivitas teknis, melainkan tindakan hukum yang harus mempertimbangkan tujuan, penerima, keamanan, dan kepatuhan terhadap prinsip perlindungan. Portabilitas dan interoperabilitas merupakan isu yang berbeda tetapi saling berhubungan. Portabilitas memberikan hak kepada subjek data untuk memperoleh atau memindahkan data dalam kondisi tertentu, sedangkan interoperabilitas menyangkut kemampuan sistem berbeda untuk bertukar data dengan format dan standar yang kompatibel. Wiwoho et al. (2024) menunjukkan bahwa hak portabilitas membutuhkan pedoman standar dan arsitektur teknis.

Perbandingan dengan GDPR memberikan ilustrasi mengenai pentingnya mekanisme transfer dan pengawasan yang terstruktur. GDPR mengatur pemrosesan data pribadi dan menyediakan kerangka hak individu serta kewajiban organisasi (European Parliament & Council of the European Union, 2016). Indonesia perlu mengembangkan mekanisme yang sesuai dengan struktur hukum dan kapasitas kelembagaannya. Pada level praktis, organisasi perlu membuat pemetaan aliran data: dari mana data berasal, untuk tujuan apa dikumpulkan, siapa yang mengakses, di mana disimpan, kapan dihapus, dan kepada siapa dapat ditransfer. Data mapping menghubungkan kewajiban hukum dengan pengendalian teknis.

F. Tantangan Kelembagaan dan Kepastian Hukum

Keberadaan undang-undang tidak otomatis menghasilkan perlindungan efektif. Implementasi memerlukan kelembagaan pengawas yang memiliki kewenangan, sumber daya, kompetensi teknis, dan prosedur yang dapat diprediksi. Literatur mengenai pembentukan otoritas perlindungan data di Indonesia menunjukkan bahwa desain kelembagaan berkaitan dengan efektivitas sanksi dan penyelesaian sengketa.

Tantangan berikutnya adalah kepastian aturan pelaksana. Firdaus (2024) menunjukkan bahwa ketentuan yang belum cukup konkret dapat menciptakan ketidakpastian bagi pengendali data. Dari sisi subjek data, ketidakpastian dapat mempersulit pemahaman mengenai bagaimana hak harus diajukan. Implementasi juga memerlukan literasi hukum dan teknis. Tidak semua organisasi memiliki kapasitas yang sama untuk menerapkan inventarisasi data, penilaian risiko, pengamanan, audit, dan respons insiden. Kepatuhan perlu memperhatikan ukuran dan karakter organisasi tanpa mengurangi standar perlindungan yang diwajibkan hukum.

Razi et al. (2024) mengidentifikasi tantangan implementasi UU PDP melalui isu kebocoran data, regulasi, keamanan siber, dan perbandingan dengan aturan internasional. Perlindungan data merupakan persoalan lintas bidang: hukum menetapkan kewajiban, teknologi menyediakan kontrol, manajemen mengatur proses, dan pengguna perlu memahami hak serta risiko.

Supeno et al. (2025) menunjukkan pentingnya mekanisme penyelesaian sengketa dan kelembagaan khusus. Mekanisme tersebut perlu memberikan akses yang wajar kepada subjek data, menyediakan proses transparan, dan memungkinkan pemulihan ketika hak dilanggar.

G. Model Penguatan Implementasi Perlindungan Data

Berdasarkan analisis norma dan literatur, penguatan implementasi dapat dibangun melalui hubungan antara tiga lapisan: tata kelola, teknologi, dan penegakan hukum. Tata kelola memastikan organisasi mengetahui tujuan pemrosesan, kategori data, dasar pemrosesan, masa retensi, serta pihak yang terlibat. Teknologi memastikan akses dan penggunaan data dapat dikendalikan. Penegakan hukum memastikan pelanggaran dapat ditangani dan hak subjek data dapat dipulihkan.

Pada lapisan tata kelola, organisasi perlu mengembangkan inventaris pemrosesan data dan kebijakan retensi. Data yang tidak lagi memiliki tujuan yang sah seharusnya tidak disimpan tanpa batas. Prinsip pembatasan penyimpanan memiliki hubungan erat dengan keamanan karena data yang sudah tidak diperlukan tetap dapat menjadi target akses tidak sah.

Tabel 2 Model Penguatan Implementasi

Lapisan	Fokus Penguatan	Contoh Tindakan
Tata Kelola	Inventarisasi dan retensi	Data mapping, klasifikasi, kebijakan retensi, dan dokumentasi dasar pemrosesan.
Teknologi	Privacy by design dan keamanan	Enkripsi, kontrol akses, autentikasi, logging, dan pengujian keamanan.
Penegakan	Pengaduan dan respons insiden	Jalur pengaduan, notifikasi, pemulihan, audit, dan evaluasi kepatuhan.

Pada lapisan teknologi, pendekatan *privacy by design* dapat digunakan sejak tahap perancangan. Contohnya adalah penggunaan akses berbasis peran, enkripsi, autentikasi berlapis, pemisahan lingkungan produksi dan pengujian, serta pencatatan aktivitas. Teknologi bukan pengganti kewajiban hukum, tetapi instrumen untuk mengurangi kemungkinan dan dampak pelanggaran.

Pada lapisan penegakan, diperlukan prosedur pengaduan dan respons insiden yang jelas. Organisasi harus memiliki jalur internal untuk menerima permintaan subjek data dan mencatat penyelesaiannya. Pengawas perlu memiliki indikator yang memungkinkan evaluasi kepatuhan secara konsisten.

Dalam sektor finansial, penggunaan data biometrik dan *Electronic Know Your Customer* (e-KYC) perlu mendapat perhatian lebih karena kegagalan pemrosesan dapat berdampak pada identitas dan akses seseorang terhadap layanan. Fitriyanti et al. (2024) menunjukkan bahwa *Electronic Know Your Customer* (e-KYC) telah menjadi bagian transformasi layanan finansial sekaligus memerlukan perlindungan data. Pada e-commerce, pemetaan transfer data dan hubungan dengan pihak ketiga juga penting.

Model tersebut menunjukkan bahwa keberhasilan UU PDP tidak dapat hanya dinilai dari keberadaan norma. Implementasi perlu dilihat dari kemampuan organisasi menerapkan prinsip secara operasional, kemampuan individu menggunakan haknya, dan kemampuan lembaga pengawas memastikan kepatuhan. Syailendra et al. (2024) juga menempatkan tahap implementasi sebagai tantangan penting setelah lahirnya UU PDP.

H. Dasar Pemrosesan, Persetujuan, dan Transparansi

Keberlakuan prinsip perlindungan data tidak dapat dilepaskan dari pertanyaan mengenai dasar pemrosesan. Dalam praktik layanan digital, persetujuan sering dipahami sebagai bentuk penerimaan pengguna terhadap seluruh syarat layanan. Padahal, persetujuan yang bermakna menuntut adanya informasi yang cukup mengenai tujuan pemrosesan, kategori data yang diproses, pihak yang terlibat, dan konsekuensi yang mungkin timbul. Karena itu, tata kelola persetujuan perlu ditempatkan sebagai bagian dari akuntabilitas, bukan sekadar formalitas administratif.

Transparansi juga perlu dibedakan dari sekadar menyediakan kebijakan privasi. Dokumen yang panjang dan sulit dipahami belum tentu memberikan transparansi yang efektif. Informasi harus disampaikan pada saat yang relevan, menggunakan bahasa yang dapat dipahami, dan menjelaskan perubahan tujuan pemrosesan apabila terjadi. Dalam konteks aplikasi digital, transparansi dapat diwujudkan melalui pemberitahuan berlapis, ringkasan informasi, pengaturan privasi yang mudah ditemukan, serta mekanisme untuk menarik atau memperbarui pilihan pengguna sesuai dasar pemrosesan yang digunakan.

Persoalan persetujuan menjadi lebih kompleks ketika layanan memiliki ketergantungan tinggi terhadap data. Pengguna dapat secara praktis merasa tidak memiliki pilihan karena layanan hanya dapat digunakan setelah seluruh persyaratan diterima. Situasi ini menunjukkan pentingnya membedakan antara persetujuan yang benar-benar diberikan secara bebas dan penerimaan terhadap syarat penggunaan layanan. Analisis hukum harus melihat konteks hubungan para pihak, tujuan pemrosesan, jenis data, dan keseimbangan kepentingan yang terlibat.

Pendekatan tersebut sejalan dengan gagasan akuntabilitas. Pengendali bukan hanya dituntut menunjukkan bahwa suatu proses pernah disetujui, tetapi juga harus dapat menjelaskan mengapa data tertentu diperlukan, bagaimana data tersebut digunakan, siapa yang memperoleh akses, dan kapan data akan dihapus. Dokumentasi keputusan menjadi penting karena dapat digunakan untuk membuktikan kepatuhan apabila muncul pemeriksaan, sengketa, atau permintaan dari subjek data.

I. Retensi, Penghapusan, dan Minimisasi Data

Prinsip minimisasi data mempunyai hubungan langsung dengan kebijakan retensi. Semakin banyak data dikumpulkan dan semakin lama disimpan, semakin besar pula ruang risiko yang harus dikelola oleh organisasi. Oleh sebab itu, pemrosesan yang bertanggung jawab perlu dimulai dengan pertanyaan apakah setiap kategori data memang diperlukan untuk tujuan tertentu. Jika suatu data tidak lagi relevan, organisasi perlu memiliki dasar dan prosedur yang jelas untuk menghapus atau memusnahkannya sesuai ketentuan yang berlaku.

Dalam praktik, kebijakan retensi tidak cukup dibuat dalam satu dokumen umum. Organisasi perlu menghubungkan masa penyimpanan dengan jenis data, tujuan pemrosesan, kewajiban hukum, kebutuhan pembuktian, serta risiko keamanan. Data identitas pelanggan, catatan transaksi, rekaman komunikasi, dan data biometrik dapat memiliki kebutuhan retensi yang berbeda. Pemetaan tersebut membuat organisasi dapat menentukan siapa yang bertanggung jawab atas penghapusan, sistem mana yang harus dibersihkan, dan bagaimana memastikan salinan cadangan tidak diabaikan.

Masalah penghapusan juga berkaitan dengan penggunaan penyedia layanan pihak ketiga. Data yang sudah dihapus dari sistem utama dapat tetap berada pada penyedia cloud, sistem analitik, arsip, atau cadangan. Karena itu, kontrak dan prosedur teknis perlu mengatur siklus hidup data secara menyeluruh. Akuntabilitas tidak berhenti ketika data keluar dari sistem utama; pengendali perlu memahami rantai pemrosesan yang terjadi setelah data dibagikan kepada prosesor atau pihak lain.

Dari sudut pandang hak subjek data, mekanisme penghapusan harus dapat digunakan secara realistis. Permintaan tidak boleh berhenti pada formulir pengaduan tanpa kepastian mengenai waktu pemeriksaan, verifikasi identitas, keputusan, dan tindak lanjut. Prosedur yang jelas juga membantu organisasi membedakan permintaan yang wajib dipenuhi dari keadaan ketika penyimpanan masih diwajibkan oleh hukum atau diperlukan untuk tujuan tertentu yang sah.

J. Sanksi, Pengawasan, dan Penyelesaian Sengketa

Kerangka perlindungan data akan memiliki daya guna yang lebih kuat apabila terdapat mekanisme pengawasan dan pertanggungjawaban yang dapat dijalankan. UU PDP tidak hanya mengatur hak dan kewajiban, tetapi juga menyediakan konsekuensi hukum terhadap pelanggaran tertentu. Dalam konteks implementasi, keberadaan sanksi perlu diikuti dengan prosedur pemeriksaan yang transparan sehingga pelaku usaha maupun subjek data mengetahui bagaimana suatu pelanggaran dinilai dan bagaimana hak untuk memberikan penjelasan dapat digunakan. Pengawasan juga perlu memperhatikan karakter risiko. Tidak semua pemrosesan data mempunyai dampak yang sama. Pemrosesan data untuk layanan dasar dengan kategori data terbatas memiliki profil risiko yang berbeda dari pemrosesan biometrik, profil perilaku, atau data yang digunakan untuk mengambil keputusan yang berdampak signifikan terhadap seseorang. Pendekatan berbasis risiko membantu organisasi memprioritaskan sumber daya pada proses yang paling membutuhkan pengamanan dan pengawasan.

Penyelesaian sengketa menjadi bagian penting dari perlindungan hak. Subjek data membutuhkan saluran yang mudah diakses untuk mempertanyakan penggunaan datanya, sedangkan organisasi memerlukan prosedur internal untuk menerima, memverifikasi, mencatat, dan menyelesaikan permintaan. Mekanisme tersebut sebaiknya menghasilkan jejak audit yang dapat menunjukkan kapan permintaan diterima, siapa yang memproses, dasar keputusan, dan tindakan korektif yang dilakukan. Dalam perspektif hukum, mekanisme penyelesaian sengketa juga berfungsi sebagai umpan balik untuk memperbaiki tata kelola. Pola pengaduan yang berulang dapat menunjukkan kelemahan pada desain layanan, pemberitahuan privasi, pengaturan akses, atau kebijakan retensi. Dengan demikian, penanganan sengketa tidak hanya bersifat reaktif, tetapi dapat digunakan sebagai instrumen perbaikan berkelanjutan.

K. Penerapan pada Sektor Digital dan Keuangan

Penerapan perlindungan data terlihat jelas pada layanan keuangan digital karena proses bisnisnya membutuhkan identitas, informasi kontak, riwayat transaksi, dan dalam kondisi tertentu data biometrik. Fitriyanti et al. (2024) menempatkan keamanan data dalam proses e-KYC sebagai unsur penting bagi perkembangan ekonomi digital. Hal ini menunjukkan bahwa kepatuhan tidak cukup dilihat dari tersedianya persetujuan, tetapi juga dari bagaimana identitas diverifikasi, bagaimana data disimpan, dan bagaimana akses diberikan kepada pihak yang membutuhkan.

Dalam pinjaman daring, penggunaan data dapat meluas dari verifikasi identitas hingga penilaian kelayakan dan pengelolaan risiko. Dewi dan Sulistyawan (2024) membahas perlindungan data pribadi nasabah dalam transaksi pinjaman online. Dari perspektif tata kelola, organisasi perlu membatasi akses berdasarkan fungsi, mendokumentasikan tujuan pemrosesan, dan memastikan bahwa penggunaan data tidak berkembang menjadi tujuan lain tanpa dasar yang memadai.

Pada sektor perdagangan elektronik, persoalan transfer data menjadi lebih menonjol karena transaksi melibatkan penjual, penyedia pembayaran, logistik, platform, penyedia cloud, dan mitra analitik. Marischa dan Setianingrum (2024) mengkaji transfer data oleh perusahaan e-commerce dari perspektif hukum perlindungan data Indonesia. Struktur rantai tersebut memperlihatkan pentingnya data mapping agar organisasi dapat mengetahui aliran data dari titik pengumpulan sampai kepada pihak penerima.

Kasus-kasus sektoral tersebut menunjukkan bahwa implementasi UU PDP membutuhkan pendekatan yang kontekstual. Prinsip hukumnya bersifat umum, tetapi prosedur teknis harus disesuaikan dengan jenis layanan, kategori data, risiko, dan struktur hubungan para pihak. Karena itu,

kebijakan internal yang hanya menyalin istilah undang-undang tanpa menerjemahkannya menjadi kontrol operasional belum cukup untuk membuktikan kepatuhan secara substantif.

L. Perbandingan Terbatas dengan GDPR

Perbandingan dengan GDPR berguna sebagai bahan analisis karena keduanya sama-sama menempatkan hak subjek data, prinsip pemrosesan, keamanan, dan akuntabilitas sebagai unsur penting. Namun, perbandingan tidak berarti bahwa ketentuan Eropa dapat diterapkan begitu saja di Indonesia. Sistem hukum, kelembagaan, struktur industri, dan karakter layanan digital Indonesia memiliki konteks tersendiri. Salah satu persamaan penting adalah perhatian terhadap keterbukaan tujuan pemrosesan dan posisi subjek data. GDPR memberikan kerangka rinci mengenai prinsip pemrosesan, hak individu, kewajiban pengendali dan prosesor, serta mekanisme transfer. UU PDP juga membangun elemen-elemen yang serupa dalam sistem hukum Indonesia. Perbandingan tersebut membantu menunjukkan bahwa isu perlindungan data bukan hanya persoalan kerahasiaan, tetapi juga menyangkut kontrol individu, akuntabilitas organisasi, dan tata kelola siklus hidup data. Perbedaan dapat muncul dalam cara aturan diterapkan dan kelembagaan yang menjalankannya. Efektivitas suatu norma bergantung pada kapasitas pengawasan, prosedur administratif, budaya kepatuhan, dan kesiapan organisasi. Karena itu, ukuran keberhasilan tidak semestinya hanya menggunakan keberadaan norma tertulis, tetapi juga melihat apakah hak dapat dijalankan, apakah pengendali mampu membuktikan kepatuhan, dan apakah pelanggaran dapat ditangani secara konsisten. Dengan pendekatan tersebut, pengalaman GDPR dapat digunakan sebagai bahan pembelajaran tanpa menghilangkan karakter sistem hukum nasional. Indonesia dapat mengambil pelajaran mengenai dokumentasi, privacy by design, pengelolaan risiko, dan tata kelola transfer data, lalu menyesuaikannya dengan kebutuhan dan kerangka hukum domestik. Perbandingan yang proporsional membantu menghindari dua ekstrem, yaitu menganggap hukum Indonesia sepenuhnya berbeda sehingga tidak perlu belajar dari praktik internasional, atau sebaliknya menyalin model asing tanpa penyesuaian.

M. Data Governance dan Akuntabilitas Organisasi

Tata kelola data merupakan jembatan antara kewajiban hukum dan praktik organisasi. Organisasi yang memproses data dalam jumlah besar memerlukan inventarisasi mengenai kategori data, sumber data, tujuan pemrosesan, sistem yang digunakan, pihak yang menerima akses, dan masa penyimpanan. Inventaris tersebut membantu memastikan bahwa setiap kegiatan pemrosesan dapat ditelusuri. Tanpa pemetaan, organisasi akan kesulitan menentukan siapa yang bertanggung jawab ketika terjadi kesalahan, kebocoran, atau permintaan penghapusan. Akuntabilitas juga menuntut adanya pembagian tanggung jawab internal. Fungsi teknologi informasi, keamanan, hukum, kepatuhan, pemasaran, dan layanan pelanggan dapat bersentuhan dengan data pribadi dengan cara yang berbeda. Karena itu, kebijakan perlindungan data perlu diterjemahkan menjadi prosedur yang spesifik untuk setiap fungsi. Misalnya, bagian pemasaran perlu mengetahui batas penggunaan data untuk komunikasi promosi, sedangkan tim teknologi perlu memahami standar akses, pencatatan, dan pengamanan sistem. Kontrak dengan prosesor dan pihak ketiga merupakan bagian lain dari akuntabilitas. Hubungan kontraktual sebaiknya tidak berhenti pada klausul umum mengenai kerahasiaan, tetapi mengatur tujuan pemrosesan, instruksi pengendali, jenis data, pengamanan, subprosesor, pemberitahuan insiden, penghapusan atau pengembalian data, serta mekanisme audit. Pendekatan tersebut membuat rantai pemrosesan menjadi lebih transparan dan mengurangi ketidakjelasan mengenai pihak yang harus bertindak ketika terjadi insiden. Akuntabilitas pada akhirnya perlu dibuktikan melalui dokumentasi. Catatan pemrosesan, hasil penilaian risiko, keputusan mengenai retensi, catatan pelatihan, hasil pengujian keamanan, dan bukti penanganan permintaan subjek data dapat menjadi indikator bahwa organisasi tidak hanya memiliki kebijakan di atas kertas. Dokumentasi juga membantu organisasi melakukan evaluasi berkala ketika layanan, teknologi, atau tujuan bisnis berubah.

N. Penilaian Risiko dan Privacy by Design

Pendekatan berbasis risiko memungkinkan organisasi menyesuaikan tingkat pengamanan dengan karakter pemrosesan. Risiko dapat dinilai dengan melihat jenis data, jumlah subjek data, skala pemrosesan, kemungkinan penyalahgunaan, dampak apabila terjadi kebocoran, serta ketergantungan individu terhadap layanan. Data biometrik, misalnya, memiliki karakter yang berbeda dari data kontak biasa karena perubahan atau penggantian atribut tersebut tidak semudah mengganti kata sandi.

Penilaian risiko sebaiknya dilakukan sebelum sistem baru diluncurkan dan diulang ketika terjadi perubahan penting. Perubahan algoritma, integrasi dengan pihak ketiga, penggunaan teknologi kecerdasan buatan, atau perluasan tujuan pemrosesan dapat mengubah profil risiko. Dengan evaluasi berkala, organisasi dapat mengidentifikasi kebutuhan pengamanan baru sebelum risiko tersebut berubah menjadi insiden yang nyata.

Konsep privacy by design memperkuat pendekatan tersebut dengan memasukkan perlindungan data sejak tahap desain. Sistem sebaiknya tidak dirancang untuk mengumpulkan semua informasi yang mungkin berguna pada masa depan. Sebaliknya, pengembang perlu mempertanyakan data apa yang benar-benar dibutuhkan, siapa yang perlu mengaksesnya, berapa lama data disimpan, dan bagaimana pengguna dapat mengendalikan informasi mengenai dirinya.

Penerapan privacy by design juga dapat menghasilkan manfaat operasional. Pembatasan akses sejak awal mengurangi kebutuhan melakukan koreksi setelah sistem berjalan. Pengaturan retensi otomatis dapat mengurangi data yang tersimpan tanpa tujuan. Logging dan pemantauan dapat membantu mendeteksi penggunaan yang tidak wajar. Dengan demikian, perlindungan data bukan semata-mata beban kepatuhan, tetapi dapat menjadi bagian dari desain sistem yang lebih tertib dan dapat diaudit.

O. Arah Penguatan Implementasi

Penguatan implementasi UU PDP membutuhkan koordinasi antara pembentuk kebijakan, lembaga pengawas, organisasi pengendali dan prosesor, serta masyarakat sebagai subjek data. Norma yang baik membutuhkan petunjuk pelaksanaan yang cukup jelas, sementara organisasi memerlukan kapasitas untuk menerjemahkan kewajiban menjadi prosedur. Di sisi lain, masyarakat membutuhkan literasi agar mampu mengenali hak, membaca pemberitahuan privasi, dan menggunakan mekanisme pengaduan secara efektif.

Dari sisi organisasi, prioritas awal dapat diarahkan pada pemetaan pemrosesan dan identifikasi risiko. Setelah itu, organisasi dapat menyusun kebijakan retensi, memperkuat kontrol akses, memperbaiki prosedur penanganan permintaan subjek data, dan menguji rencana respons insiden. Urutan tersebut membantu organisasi menghindari pendekatan administratif yang hanya menghasilkan dokumen tanpa perubahan pada praktik pemrosesan. Dari sisi pengawasan, pendekatan berbasis risiko dapat membantu mengarahkan perhatian pada pemrosesan yang memiliki dampak lebih besar terhadap hak individu. Pengawasan juga dapat mendorong kepatuhan preventif melalui pedoman, edukasi, dan mekanisme konsultasi, selain tindakan setelah terjadi pelanggaran. Keseimbangan antara pencegahan dan penegakan penting agar organisasi memiliki insentif untuk memperbaiki tata kelola sebelum terjadi kerugian.

Bagi subjek data, penguatan implementasi harus terlihat dalam pengalaman penggunaan layanan. Informasi mengenai pemrosesan harus mudah ditemukan, permintaan hak harus memiliki jalur yang jelas, dan respons organisasi harus dapat dipertanggungjawabkan. Dengan demikian, keberhasilan perlindungan data dapat dilihat tidak hanya dari jumlah kebijakan atau dokumen kepatuhan, tetapi dari kemampuan sistem hukum dan organisasi memberikan kontrol yang nyata kepada individu.

P. Peran Literasi dan Kepatuhan Internal

Pelindungan data pribadi tidak hanya bergantung pada unit hukum atau keamanan informasi. Setiap pegawai yang memperoleh akses terhadap data dapat menjadi bagian dari rantai pemrosesan. Karena itu, organisasi perlu membangun literasi internal yang menjelaskan jenis data yang boleh diakses, tujuan penggunaan, batas pengungkapan, tata cara penyimpanan, serta langkah yang harus dilakukan ketika terjadi kesalahan atau dugaan insiden. Pelatihan perlu disesuaikan dengan fungsi pekerjaan sehingga tidak berhenti pada penjelasan normatif yang terlalu umum. Kepatuhan internal juga perlu diuji secara berkala. Audit dapat dilakukan dengan mengambil sampel proses untuk melihat apakah data yang dikumpulkan sesuai dengan tujuan, apakah hak akses masih relevan, apakah data yang sudah melewati masa retensi masih tersimpan, dan apakah permintaan subjek data telah ditangani sesuai prosedur. Hasil audit sebaiknya diterjemahkan menjadi tindakan korektif dengan penanggung jawab dan batas waktu yang jelas. Dengan demikian, kepatuhan menjadi siklus perbaikan, bukan kegiatan satu kali.

Budaya organisasi berpengaruh terhadap efektivitas pengendalian. Ketika kecepatan peluncuran layanan selalu ditempatkan di atas pertimbangan privasi, kontrol yang telah dibuat dapat

dilewati dalam praktik. Sebaliknya, apabila perlindungan data dimasukkan dalam proses persetujuan perubahan sistem, pengadaan teknologi, dan evaluasi vendor, risiko dapat dipertimbangkan lebih awal. Akuntabilitas karena itu perlu ditempatkan sebagai bagian dari pengambilan keputusan organisasi sehari-hari.

Q. Implikasi bagi Subjek Data dan Pengguna Layanan

Bagi subjek data, kerangka hukum memberikan dasar untuk meminta informasi dan menggunakan hak atas data yang berkaitan dengannya. Namun, hak akan sulit digunakan apabila pengguna tidak mengetahui siapa pengendali datanya, untuk apa data digunakan, dan bagaimana cara mengajukan permintaan. Informasi tersebut seharusnya tersedia pada titik ketika data dikumpulkan dan tetap dapat diakses selama hubungan layanan berlangsung. Pengguna juga perlu memahami bahwa keamanan data merupakan tanggung jawab bersama yang tidak seluruhnya dapat dialihkan kepada organisasi. Penggunaan kata sandi yang kuat, autentikasi berlapis, kehati-hatian terhadap tautan atau permintaan informasi yang mencurigakan, dan pemahaman terhadap pengaturan privasi dapat mengurangi risiko tertentu. Meski demikian, kewaspadaan pengguna tidak menghapus kewajiban pengendali untuk menyediakan sistem yang aman dan tata kelola yang sesuai dengan hukum. Hubungan antara hak pengguna dan kewajiban organisasi menunjukkan bahwa perlindungan data merupakan mekanisme timbal balik. Organisasi harus membangun sistem yang memungkinkan kontrol individu, sedangkan pengguna perlu memanfaatkan informasi dan mekanisme yang tersedia. Apabila salah satu sisi tidak berjalan, tujuan perlindungan menjadi kurang efektif. Karena itu, peningkatan literasi publik perlu berjalan bersama dengan peningkatan kepatuhan organisasi.

Secara keseluruhan, pembahasan tersebut memperlihatkan bahwa UU PDP menyediakan fondasi hukum, tetapi efektivitasnya ditentukan oleh penerjemahan norma ke dalam prosedur yang dapat digunakan. Hak, keamanan, dokumentasi, retensi, pengawasan, dan penyelesaian sengketa harus dipandang sebagai satu rangkaian. Pendekatan yang terintegrasi membantu mencegah pemrosesan data dilakukan tanpa tujuan yang jelas sekaligus memberikan jalur pemulihan ketika terjadi pelanggaran.

R. Integrasi Kebijakan, Teknologi, dan Penegakan

Analisis keseluruhan memperlihatkan bahwa perlindungan data tidak dapat ditempatkan hanya pada satu lapisan kebijakan. Norma hukum menetapkan hak dan kewajiban, tata kelola menerjemahkannya menjadi prosedur, sedangkan teknologi menyediakan sarana untuk menjalankan dan mengawasi prosedur tersebut. Ketiganya perlu saling mendukung. Kebijakan yang baik tanpa kontrol teknis akan sulit diterapkan, sedangkan kontrol teknis tanpa dasar kebijakan dapat menghasilkan pengumpulan atau pembatasan akses yang tidak memiliki tujuan hukum yang jelas.

Integrasi tersebut dapat dimulai dari proses pengadaan dan pengembangan layanan. Setiap proyek baru yang memproses data sebaiknya memiliki tahapan untuk mengidentifikasi tujuan, kategori data, pihak yang menerima akses, risiko, kebutuhan retensi, serta mekanisme pemenuhan hak. Hasil penilaian tersebut kemudian dapat digunakan sebagai persyaratan teknis dan kontraktual. Dengan cara ini, perlindungan data menjadi bagian dari siklus hidup layanan sejak awal, bukan tindakan korektif setelah sistem selesai dibangun.

Pada tahap operasional, organisasi perlu melakukan pemantauan dan evaluasi. Perubahan tujuan bisnis, integrasi dengan vendor baru, perpindahan penyimpanan, atau penggunaan teknologi baru dapat mengubah risiko. Evaluasi berkala memastikan bahwa kebijakan yang semula sesuai tetap relevan. Dokumentasi perubahan juga penting agar organisasi dapat menjelaskan alasan keputusan dan menunjukkan bahwa pengelolaan data dilakukan secara sadar serta dapat dipertanggungjawabkan.

Kerangka tersebut memberikan dasar untuk memahami keberhasilan implementasi secara lebih utuh. Ukuran keberhasilan tidak cukup berupa keberadaan kebijakan privasi atau jumlah pelatihan, tetapi perlu dilihat dari apakah hak subjek data dapat dijalankan, apakah akses terhadap data dapat dikendalikan, apakah insiden dapat dideteksi dan ditangani, serta apakah data yang tidak lagi diperlukan benar-benar dikelola sesuai kebijakan. Dengan ukuran tersebut, perlindungan data dapat diposisikan sebagai proses tata kelola yang berkelanjutan.

Penguatan implementasi juga perlu memperhatikan konsistensi antara kebijakan pusat dan prosedur pada unit operasional. Dalam organisasi besar, kebijakan yang sama dapat diterapkan oleh banyak tim dengan tingkat pemahaman yang berbeda. Standar minimum, matriks tanggung jawab, dan jalur eskalasi membantu mengurangi perbedaan penerapan. Dokumentasi keputusan penting juga dapat

mencegah perubahan prosedur yang tidak tercatat ketika terjadi pergantian personel atau penyedia teknologi.

Aspek lain yang perlu diperhatikan adalah hubungan antara perlindungan data dan keberlanjutan layanan. Ketika terjadi insiden, organisasi harus mampu mengamankan sistem sekaligus menjaga layanan penting tetap berjalan secara proporsional. Rencana respons insiden karena itu perlu memuat pembagian peran, prioritas pemulihan, mekanisme komunikasi, serta evaluasi setelah insiden selesai. Evaluasi pascainsiden penting untuk menemukan akar masalah dan memperbaiki kontrol yang sebelumnya tidak memadai.

Dengan demikian, penerapan UU PDP dapat dipahami sebagai proses membangun tata kelola yang dapat diuji. Prinsip hukum harus terlihat dalam desain layanan, prosedur internal, kontrak dengan pihak ketiga, pengamanan teknologi, serta pengalaman subjek data ketika menggunakan haknya. Kerangka semacam ini membuat perlindungan data tidak berhenti pada kepatuhan formal, tetapi menjadi bagian dari cara organisasi mengelola informasi sepanjang siklus hidupnya.

KESIMPULAN

Undang-Undang Nomor 27 Tahun 2022 telah memberikan dasar hukum yang lebih terintegrasi dalam perlindungan data pribadi di Indonesia melalui pengaturan hak subjek data, kewajiban pengendali dan prosesor, keamanan, serta pertanggungjawaban pemrosesan data. Namun, tantangan utama masih terletak pada implementasi, khususnya dalam kepastian hukum, pengelolaan hak subjek data, keamanan, transfer data, dan penegakan hukum. Oleh karena itu, diperlukan penguatan tata kelola, teknologi, dan kelembagaan melalui pemetaan aliran data, pengamanan berbasis risiko, prosedur respons insiden, serta peningkatan kapasitas pengawasan dan literasi. Kerangka perlindungan data juga perlu terus dievaluasi dan disesuaikan dengan perkembangan teknologi, seperti kecerdasan buatan, biometrik, komputasi awan, dan transfer data lintas batas, agar perlindungan privasi tetap efektif dan berkelanjutan.

DAFTAR PUSTAKA

- Dewi, S. P., & Sulistyawan, A. Y. (2024). Perlindungan hukum data pribadi nasabah dalam transaksi pinjaman online. *Notarius*, 17(3), 2265–2282.
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
- Fauzy, E., & Shandy, N. A. R. (2023). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3).
- Firdaus, F. H. (2024). Perlindungan dan kepastian hukum bagi pengendali data pribadi di masa depan. *Masalah-Masalah Hukum*, 53(2), 135–144.
- Fitriyanti, F., Devty, S., Putri, S., & Thora, R. E. (2024). Securing personal data in e-KYC: Vital for digital economy growth. *Diponegoro Law Review*, 9(1), 104–120.
- Human Rights Council. (2023). The right to privacy in the digital age: Resolution 54/21. United Nations.
- Human Rights Council. (2024). Mandate of the Special Rapporteur on the right to privacy: Resolution 55/3. United Nations.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems Requirements. ISO.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2016). Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
- Marischa, D., & Setianingrum, R. B. (2024). Transfer of personal data by e-commerce companies: A study from the perspective of Indonesian personal data protection laws. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 4(1), 48–64.
- Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. OECD Publishing.

- Pratiwi, B., Fadilla, N. N., Syawal, I. N., & Zholanda. (2025). The implementation of personal data protection policy within Indonesia's digital legal system. *Perkara: Jurnal Ilmu Hukum dan Politik*.
- Razi, F., Tuasikal, H., & Pratiwi Markus, D. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(12), 6559–6565.
- Republik Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Republik Indonesia. (2008). Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. (2016). Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Republik Indonesia. (2019). Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
- Republik Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Rosadi, S. D., et al. (2023). Indonesia's personal data protection bill, 2020: Does it meet the needs of the new digital economy? *International Review of Law, Computers & Technology*, 37(1), 78–90.
- Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–134.
- Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal data protection in review of legal theories and principles. *Journal of Law and Legal Reform*, 6(3).
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, 14(2).
- United Nations General Assembly. (2013). The right to privacy in the digital age (A/RES/68/167). United Nations.
- United Nations General Assembly. (2017). The right to privacy in the digital age (A/RES/72/179). United Nations.
- United Nations. (1948). Universal Declaration of Human Rights. United Nations.
- Wiwoho, J., Pati, U. K., & Pratama, A. M. (2024). Enabling data portability and interoperability under Indonesia's data protection law. *Masalah-Masalah Hukum*, 53(3), 271–282.
- Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta Research Law Journal*, 19(2).