OPTIMALISASI PELINDUNGAN DATA PRIBADI KONSUMEN MELALUI PENGUATAN MEKANISME AUDIT KEPATUHAN SEBAGAI UPAYA MEWUJUDKAN KEPASTIAN HUKUM DALAM TRANSAKSI DIGITAL DI INDONESIA

Oleh: **Lintang Ayudyaningrum**
Universitas Negeri Jakarta, Jl. R.M. Mangun Muka Raya No 11, Rawamangun, Kec. Pulo Gadung, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13220, Indonesia.
email: lintang.ayudya07@gmail.com

Informasi Artikel *Received*: 09-08-2026 **Accepted:** 25-10-2026

ABSTRAK

Transformasi digital telah mendorong peningkatan penggunaan perdagangan elektronik, layanan keuangan digital, serta berbagai *platform* berbasis teknologi yang mengandalkan pemrosesan data pribadi konsumen. Di sisi lain, tingginya angka kebocoran data pribadi yang melibatkan penyelenggara sistem elektronik menunjukkan bahwa pelindungan hukum terhadap data konsumen masih menghadapi tantangan serius. Meskipun Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, berbagai kasus kebocoran data yang terus terjadi mengindikasikan adanya kesenjangan antara keberadaan regulasi dengan efektivitas implementasinya. Kondisi tersebut berpotensi menimbulkan kerugian ekonomi, penyalahgunaan identitas, serta menurunkan tingkat kepercayaan masyarakat terhadap ekosistem transaksi digital. Penelitian ini bertujuan menganalisis efektivitas pelindungan hukum terhadap data pribadi konsumen serta merumuskan strategi penguatan kepastian hukum melalui penerapan mekanisme Audit Kepatuhan Pelindungan Data (*Data Protection Compliance Audit*) bagi penyelenggara sistem elektronik. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual, serta studi kepustakaan yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa kelemahan utama tidak terletak pada ketiadaan regulasi, melainkan pada lemahnya implementasi, pengawasan, dan akuntabilitas penyelenggara sistem elektronik dalam mengelola data pribadi. Oleh karena itu, penguatan audit kepatuhan secara berkala diperlukan sebagai instrumen preventif untuk meningkatkan kepatuhan penyelenggara sistem elektronik, melindungi hak konsumen, dan mewujudkan kepastian hukum dalam transaksi digital di Indonesia.

Kata kunci: Pelindungan Data Pribadi, Perlindungan Konsumen, Audit Kepatuhan, Hukum Bisnis, Transaksi Digital.

ABSTRACT

Optimizing the protection of consumers' personal data through Strengthening the data protection compliance audit mechanism to achieve legal certainty in digital transactions in Indonesia

Digital transformation has accelerated the growth of electronic commerce, digital financial services, and various technology-based platforms that rely on the processing of consumers' personal data. On the other hand, the increasing number of personal data breaches involving electronic system providers indicate that legal protection for consumers' personal data continues to face significant challenges. Although Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection, the persistence of data breach cases reflects a gap between the existence of the legal framework and the effectiveness of its implementation. This condition may result in economic losses, identity misuse, and a decline in public trust in the digital transaction ecosystem. This study aims to analyze the effectiveness of legal protection for consumers' personal data and to formulate a strategy for strengthening legal certainty through the implementation of a Data Protection Compliance Audit mechanism for electronic system providers. This research employs a normative juridical method using statutory and conceptual approaches and a literature review analyzed qualitatively. The findings indicate that the primary issue lies not in the absence of regulations, but in the weak implementation, supervision, and accountability of electronic system providers in managing personal data. Therefore, strengthening periodic compliance audits as a preventive instrument to improve electronic system providers' compliance, protect consumer rights, and achieve legal certainty in digital transactions in Indonesia.

Keywords: *Personal Data Protection, Consumer Protection, Compliance Audit, Business Law, Digital Transactions.*

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital yang berdampak signifikan terhadap berbagai aspek kehidupan, termasuk kegiatan perdagangan dan transaksi elektronik di Indonesia. Pemanfaatan *e-commerce*, layanan keuangan digital, *marketplace*, serta berbagai *platform* digital memberikan kemudahan bagi masyarakat dalam melakukan transaksi secara cepat dan efisien. Di balik kemudahan tersebut, setiap aktivitas digital melibatkan pemrosesan data pribadi pengguna, seperti nama, alamat, nomor telepon, alamat surat elektronik, hingga data keuangan yang memiliki nilai ekonomi dan memerlukan perlindungan hukum. Meningkatnya intensitas pemanfaatan data pribadi menjadikan pelindungan data sebagai aspek fundamental dalam menjamin hak privasi konsumen serta mewujudkan kepastian hukum dalam transaksi digital. Sebagai respons atas kebutuhan tersebut, Pemerintah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan

Data Pribadi (UU PDP) sebagai dasar hukum yang mengatur hak subjek data, kewajiban pengendali data, serta tanggung jawab penyelenggara sistem elektronik dalam mengelola data pribadi sesuai dengan prinsip keamanan, akuntabilitas, transparansi, dan pelindungan hak subjek data. (Indonesia, 2022). Namun keberadaan kerangka hukum tersebut belum dengan sendirinya menjamin bahwa kewajiban pelindungan data pribadi telah diterapkan secara konsisten oleh setiap penyelenggara sistem elektronik dalam praktik transaksi digital.

Peneletian terdahulu menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan langkah penting dalam memperkuat kerangka hukum pelindungan data pribadi di Indonesia. Manurung dan Thalib (2023) melalui kajian yuridis terhadap UU PDP menunjukkan bahwa pengaturan pelindungan data pribadi diperlukan untuk memberikan jaminan keamanan serta mencegah penyalahgunaan data pribadi dalam perkembangan teknologi informasi. Sementara itu, Fauzy dan Shandy (2023) menempatkan pelindungan data pribadi dalam perspektif hak atas privasi dan politik hukum, sehingga pelindungan data tidak hanya berkaitan dengan aspek teknis pengelolaan informasi, tetapi juga berkaitan dengan pemenuhan hak fundamental individu.

Meskipun demikian, keberadaan kerangka hukum tersebut belum sepenuhnya menjamin efektivitas implementasi pelindungan data pribadi. Rinjani dan Firmansyah (2025) menunjukkan bahwa implementasi UU PDP masih menghadapi hambatan berupa lemahnya penegakan hukum, persoalan kelembagaan, serta rendahnya akuntabilitas dalam penyelenggaraan pelindungan data pribadi. Temuan tersebut menunjukkan adanya kesenjangan antara norma hukum yang telah tersedia dengan mekanisme pengawasan dan kepatuhan dalam praktik. Dengan demikian, persoalan pelindungan data pribadi tidak hanya berkaitan dengan keberadaan regulasi, tetapi juga dengan kemampuan penyelenggara sistem elektronik dalam menerapkan kewajiban hukum secara konsisten dan dapat dipertanggungjawabkan.

Penelitian lain juga menunjukkan bahwa pembahasan mengenai pelindungan data pribadi masih banyak diarahkan pada aspek perlindungan hukum, tanggung jawab penyelenggara, serta penanganan permasalahan setelah terjadi pelanggaran. Dalam konteks tersebut, mekanisme evaluasi kepatuhan yang dilakukan secara preventif dan berkala masih memerlukan pengembangan lebih lanjut. Audit kepatuhan pelindungan data dapat menjadi pendekatan yang menghubungkan kewajiban hukum dengan proses evaluasi terhadap praktik pengelolaan data pribadi, sehingga potensi ketidakpatuhan dapat diidentifikasi sebelum berkembang menjadi pelanggaran.

Berdasarkan penelitian terdahulu tersebut, terdapat *research gap* berupa masih terbatasnya kajian yang secara khusus merumuskan mekanisme *Data Protection Compliance Audit* sebagai instrumen preventif untuk memastikan kepatuhan penyelenggara sistem elektronik terhadap kewajiban pelindungan data pribadi. Penelitian terdahulu telah memberikan dasar mengenai pentingnya kerangka hukum, hak atas privasi, serta sebagai hambatan implementasi UU PDP, tetapi belum secara komprehensif menghubungkan ketentuan hukum tersebut dengan mekanisme

evaluasi kepatuhan yang dilakukan secara berkala dan terdokumentasi. Oleh karena itu, penelitian ini mengisi celah tersebut dengan merumuskan penguatan *Data Protection Compliance Audit* melalui tahapan identifikasi kewajiban hukum, pemeriksaan kepatuhan, identifikasi risiko, penyusunan rekomendasi perbaikan, tindak lanjut, dan verifikasi.

Kebaruan penelitian ini terletak pada perumusan *Data Protection Compliance Audit* sebagai instrumen preventif yang menghubungkan norma hukum pelindungan data pribadi dengan mekanisme evaluasi kepatuhan secara berkala. Mekanisme tersebut diarahkan tidak hanya untuk mengidentifikasi ketidakpatuhan, tetapi juga memastikan adanya tindak lanjut dan dokumentasi hasil evaluasi sebagai bukti pemenuhan kewajiban pelindungan data. Dengan pendekatan tersebut, audit kepatuhan ditempatkan sebagai mekanisme yang dapat memperkuat akuntabilitas penyelenggara sistem elektronik sekaligus mendukung terwujudnya kepastian hukum dalam transaksi digital. Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis implementasi pelindungan data pribadi dalam transaksi digital di Indonesia serta merumuskan penguatan *Data Protection Compliance* Audit sebagai instrument preventif guna meningkatkan kepatuhan penyelenggara sistem elektronik, memperkuat pelindungan hak konsumen, dan mewujudkan kepastian hukum.

METODE

Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) untuk menganalisis pelindungan data pribadi dalam transaksi digital di Indonesia. Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan, khususnya Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta bahan hukum sekunder berupa buku, artikel ilmiah, dan hasil penelitian yang relevan dengan pelindungan data pribadi, kepastian hukum, transaksi digital, dan audit kepatuhan. Pemilihan bahan hukum dilakukan berdasarkan relevansi dengan permasalahan penelitian, keterkaitan dengan objek kajian, serta kemutakhiran sumber, khususnya literatur ilmiah yang diterbitkan dalam sepuluh tahun terakhir. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelaah dan mengiventarisasi ketentuan peraturan perundang-undangan serta literatur ilmiah yang relevan. Selanjutnya, bahan hukum dianalisis secara kualitatif melalui tahap inventarisasi, klasifikasi, interpretasi, dan analisis untuk menghubungkan ketentuan hukum dengan permasalahan implementasi pelindungan data pribadi serta merumuskan penguatan *Data Protection Compliance Audit* sebagai instrumen preventif dalam mewujudkan kepastian hukum bagi konsumen dalam transaksi digital.

HASIL DAN PEMBAHASAN

1. Implementasi Pelindungan Data Pribadi dalam Transaksi Digital di Indonesia

Pada era transformasi digital, transaksi elektronik telah menjadi bagian yang tidak terpisahkan dari aktivitas masyarakat Indonesia. Perkembangan *e-commerce*,

marketplace, layanan keuangan digital, dan berbagai *platform* berbasis teknologi informasi telah meningkatkan intensitas pengumpulan, penyimpanan, serta pengolahan data pribadi konsumen. Data pribadi tidak lagi dipandang hanya sebagai identitas individu, melainkan juga sebagai aset bernilai yang mendukung keberlangsungan layanan digital. Kondisi tersebut menuntut adanya sistem pelindungan data pribadi yang mampu memberikan jaminan keamanan serta kepastian hukum bagi setiap pengguna layanan digital.

Sebagai respons terhadap perkembangan tersebut, pemerintah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai landasan hukum yang mengatur pemrosesan data pribadi di Indonesia. Undang-Undang ini memberikan kepastian mengenai hak subjek data, kewajiban pengendali dan prosesor data, serta tanggung jawab penyelenggara sistem elektronik dalam menjaga kerahasiaan, keakuratan, dan keamanan data pribadi. Kehadiran UU PDP menjadi langkah penting dalam memperkuat tata kelola pelindungan data pribadi sekaligus menyesuaikan regulasi nasional dengan perkembangan ekosistem digital (Indonesia, 2022).

Implementasi pelindungan data pribadi dalam transaksi digital tidak hanya bergantung pada keberadaan regulasi, tetapi juga memerlukan komitmen penyelenggara sistem elektronik dalam menerapkan prinsip-prinsip pelindungan data secara konsisten. Setiap penyelenggara sistem elektronik memiliki tanggung jawab untuk memastikan bahwa pengumpulan dan pemrosesan data dilakukan secara sah, transparan, serta sesuai dengan tujuan yang telah disampaikan kepada subjek data. Selain itu, penerapan sistem keamanan informasi dan pengelolaan risiko menjadi bagian penting dalam mencegah penyalahgunaan maupun kebocoran data pribadi (Indonesia, 2022). Dengan demikian, kepatuhan terhadap kewajiban pelindungan data dapat dievaluasi secara sistematis agar penerapan norma hukum tidak berhenti pada pemenuhan administratif, tetapi benar-benar diterapkan dalam pengelolaan data pribadi.

Meskipun kerangka hukum telah tersedia, implementasi pelindungan data pribadi di Indonesia masih menghadapi berbagai tantangan. Berbagai kasus kebocoran data menunjukkan bahwa kepatuhan terhadap ketentuan pelindungan data belum diterapkan secara optimal oleh seluruh penyelenggara sistem elektronik. Kondisi tersebut mengindikasikan bahwa keberadaan regulasi belum sepenuhnya menjamin kewajiban pelindungan data dilaksanakan secara konsisten guna mewujudkan kepastian hukum dan meningkatkan kepercayaan masyarakat terhadap transaksi digital (Firdaus, 2024; Mansawan et al., 2025).

Dalam konteks audit kepatuhan, kewajiban dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dapat dijadikan dasar untuk menetapkan indikator pemeriksaan terhadap penyelenggara sistem elektronik yang melakukan pemrosesan data pribadi. Audit tidak hanya menilai keberadaan kebijakan pelindungan data, tetapi juga menilai kesesuaian pelaksanaan pemrosesan data dengan kewajiban hukum yang berlaku, termasuk pemenuhan hak subjek data,

penerapan prinsip pelindungan data, keamanan data pribadi, serta akuntabilitas pengendali dan prosesor data pribadi. Dengan demikian, ketentuan dalam UU PDP dapat diterjemahkan ke dalam indikator kepatuhan yang dapat diperiksa dan didokumentasikan secara berkala. Pendekatan tersebut memungkinkan proses audit menjadi sarana untukmengidentifikasi kesenjangan antara kewajiban normatif dengan praktik pengelolaan data pribadi dalam transaksi digital.

2. Permasalahan Implementasi Pelindungan Data Pribadi

Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah menjadi landasan hukum dalam mengatur pemrosesan data pribadi, implementasinya masih menghadapi berbagai tantangan. Berbagai kasus kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa kepatuhan penyelenggara sistem elektronik terhadap ketentuan pelindungan data belum terlaksana secara optimal. Kondisi tersebut mencerminkan bahwa keberadaan regulasi belum sepenuhnya diimbangi dengan mekanisme yang mampu memastikan pelaksanaan kewajiban pengelolaan data pribadi sesuai dengan prinsip keamanan, akuntabilitas, dan transparansi. Akibatnya, hak konsumen atas pelindungan data pribadi masih berpotensi mengalami pelanggaran (Mansawan et al., 2025; Wirayoga & Wisanjaya, 2024).

Permasalahan tersebut tidak hanya disebabkan oleh faktor teknis, tetapi juga dipengaruhi oleh lemahnya tata kelola pelindungan data di tingkat organisasi. Sebagian penyelenggara sistem elektronik masih memandang pelindungan data sebagai kewajiban administratif, bukan sebagai bagian dari manajemen risiko yang harus diterapkan secara berkelanjutan. Di sisi lain, mekanisme pengawasan terhadap kepatuhan penyelenggara sistem elektronik juga belum berjalan secara optimal sehingga potensi pelanggaran sering kali baru diketahui setelah terjadi insiden kebocoran data (Firdaus, 2024). Kondisi ini menunjukkan bahwa pendekatan yang bersifat reaktif belum mampu memberikan pelindungan hukum yang efektif bagi konsumen. Ketiadaan evaluasi kepatuhan yang dilakukan secara berkala menyebabkan kelemahan dalam pengelolaan data berpotensi tidak teridentifikasi sebelum berkembang menjadi pelanggaran.

Selain menimbulkan kerugian material maupun immaterial bagi konsumen, kebocoran data pribadi juga berdampak pada menurunnya tingkat kepercayaan masyarakat terhadap penyelenggaraan transaksi digital. Kepercayaan merupakan salah satu unsur penting dalam mendukung perkembangan ekonomi digital, sehingga setiap pelanggaran pelindungan data berpotensi menghambat pertumbuhan ekosistem digital yang sehat dan berkelanjutan. Oleh karena itu, diperlukan mekanisme yang tidak hanya berorientasi pada penegakan sanksi setelah terjadi pelanggaran, tetapi juga mampu mencegah terjadinya risiko kebocoran data melalui pengawasan dan evaluasi kepatuhan secara berkelanjutan (Aristanto et al., 2025; Nugraha & Nasyuha, 2024).

Tabel 1. Perbandingan kondisi Pelindungan Data Sebelum dan Setelah *Penguatan Data Protection Compliance Audit*

Tahap Audit	Objek yang Diperiksa	Indikator Kepatuhan	Hasil Audit	Tindak Lanjut
Identifikasi kewajibann	Kebijakan dan proses pemrosesan data pribadi	Kesesuaian dengan kewajiban UU PDP	Daftar kewajiban yang harus dipenuhi	Penyesuaian kebijakan dan prosedur
Pemeriksaan kepatuhan	Proses pengumpul-an, penggunaan, penyimpanan, dan pengungkapan data	Kesesuaian pelaksanaan dengan kewajiban hukum	Temuan kepatuhan atau ketidaksesuaian	Perbaikan terhadap temuan
Penilaian risiko	Sistem, proses, dan pihak yang terlibat dalam pemrosesan data	Tingkat risiko terhadap data pribadi	Pemetaan tingkat risiko	Penyusunan langkah mitigasi
Rekomendasi perbaikan	Temuan hasil pemeriksaan	Tingkat urgensi dan dampak ketidakpatuhan	Rekomendasi tindakan korektif	Penetapan rencana tidak lanjut
Verifikasi	Pelaksanaan tindakan korektif	Kesesuaian perbaikan dengan rekomendasi	Status penyelesaian temuan	Penutupan atau pemeriksaan lanjutan

Berdasarkan Tabel 1, penguatan *Data Protection Compliance Audit* diarahkan untuk mengubah pola pelindungan data dari pendekatan yang bersifat reaktif menjadi preventif. Evaluasi kepatuhan secara berkala memungkinkan penyelenggara sistem elektronik mengidentifikasi kelemahan dalam pengelolaan data sebelum berkembang menjadi pelanggaran. Hasil evaluasi tersebut dapat menjadi dasar bagi penyelenggara untuk melakukan perbaikan dan mendokumentasikan kepatuhan terhadap kewajiban pelindungan data sehingga mekanisme audit tidak hanya berfungsi sebagai instrumen pengawasan, tetapi juga mendukung terwujudnya kepastian hukum bagi konsumen.

Penerapan *Data Protection Compliance Audit* dilakukan melalui mekanisme yang terstruktur dan berkala. Audit pada tingkat internal dapat dilakukan oleh fungsi yang memiliki kewenangan dan kompetensi dibidang kepatuhan, pelindungan data, dan keamanan informasi, sedangkan pengawasan eksternal dilaksanakan oleh lembaga yang berwenang sesuai dengan ketentuan peraturan perundang-undangan. Objek audit meliputi kebijakan dan prosedur pemrosesan data pribadi, dasar pemrosesan, pemenuhan hak subjek data, keamanan data, pengelolaan pihak ketiga, serta penanganan insiden. Indikator pemeriksaan disusun berdasarkan kewajiban dalam UU PDP dan diterjemahkan ke dalam daftar pemeriksaan untuk mengidentifikasi kepatuhan, ketidaksesuaian, dan risiko. Hasil audit dituangkan dalam laporan

yang memuat temuan, tingkat risiko, rekomendasi tindakan korektif, pihak yang bertanggung jawab, serta tindak lanjut dan verifikasi. Dengan mekanisme tersebut, audit berfungsi sebagai siklus pengendalian yang menghubungkan identifikasi kewajiban, evaluasi kepatuhan, perbaikan, verifikasi, dan dokumentasi secara berkelanjutan.

3. Analisis Data Protection Compliance Audit sebagai Instrumen Preventif dalam Pelindungan Data Pribadi

Data Protection Compliance Audit dalam penelitian ini diposisikan sebagai mekanisme evaluasi untuk menilai kepatuhan penyelenggara sistem elektronik terhadap kewajiban pelindungan data pribadi. Audit ini tidak hanya berfokus pada pemenuhan kewajiban administratif, tetapi juga mengevaluasi efektivitas tata kelola data, sistem keamanan informasi, serta penerapan prinsip-prinsip pelindungan data dalam setiap tahapan pemrosesan data pribadi. Dengan demikian, audit kepatuhan berfungsi sebagai instrumen preventif yang mampu mengidentifikasi potensi risiko sebelum berkembang menjadi pelanggaran yang merugikan konsumen (Aristanto et al., 2025; Nugraha & Nasyuha, 2024; *International Organization for Standardization,* 2022).

Penguatan mekanisme audit dilakukan melalui beberapa tahapan yang saling berkaitan, yaitu identifikasi kewajiban hukum, pemeriksaan kepatuhan, identifikasi risiko, penyusunan rekomendasi perbaikan, dan verifikasi tindak lanjut (Aristanto et al., 2025; Nugraha & Nasyuha, 2024). Tahap identifikasi kewajiban hukum digunakan untuk memetakan ketentuan pelindungan data yang harus dipenuhi oleh penyelenggara sistem elektronik, sedangkan pemeriksaan kepatuhan dilakukan untuk menilai kesesuaian kebijakan layanan digital dan praktik pengelolaan data dengan kewajiban tersebut. Selanjutnya, risiko dan kelemahan yang ditemukan menjadi dasar penyusunan rekomendasi perbaikan yang harus ditindaklanjuti dan diverifikasi kembali. Siklus preventif yang menghubungkan norma hukum dengan praktik pengelolaan data pribadi secara berkelanjutan.

Penerapan *Data Protection Compliance Audit* dapat mendorong penyelenggara sistem elektronik untuk melakukan evaluasi secara berkala terhadap kebijakan internal, prosedur operasional, serta sistem keamanan yang digunakan dalam mengelola data pribadi (*International Organization for Standardization*, 2022) dapat digunakan sebagai standar pendukung dalam pelaksanaan *Data Protection Compliance Audit*, khususnya dalam mengevaluasi aspek keamanan informasi dan pengelolaan risiko pemrosesan data pribadi. Standar ini menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi secara berkelanjutan. Namun, penerapan *International Organization for Standardization*, 2022 tidak menggantikan kewajiban hukum berdasarkan Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi. Dalam audit kepatuhan, UU PDP tetap menjadi dasar untuk

menilai pemenuhan kewajiban hukum, sedangkan *International Organization for Standardization,* 2022 dapat digunakan sebagai standar pendukung untuk menilai penerapan pengamanan informasi dan pengelolaan risiko. Dengan demikian, kedua instrumen tersebut memiliki fungsi yang saling melengkapi dalam memperkuat kepatuhan dan akuntabilitas penyelenggara sistem elektronik. Proses evaluasi tersebut memungkinkan ditemukannya kelemahan dalam pengelolaan data sehingga perbaikan dapat dilakukan sebelum terjadi insiden kebocoran data. Dengan demikian, hasil audit tidak berhenti pada identifikasi ketidakpatuhan, tetapi harus diikuti dengan Tindakan korektif dan verifikasi terhadap pelaksanaan perbaikan.

Selain memberikan manfaat bagi penyelenggara sistem elektronik, audit kepatuhan juga memberikan pelindungan yang lebih optimal bagi konsumen. Kepastian bahwa data pribadi dikelola sesuai dengan ketentuan peraturan perundang-undangan dapat meningkatkan rasa aman masyarakat dalam menggunakan layanan digital (Mansawan et al., 2025; Wirayoga & Wisanjaya, 2024). Dokumentasi hasil audit juga dapat menjadi dasar untuk menunjukkan bahwa penyelenggara telah melakukan upaya pemenuhan kewajiban pelindungan data secara terukur dan terdokumentasi. Di sisi lain, penyelenggara sistem elektronik juga memperoleh manfaat berupa peningkatan kredibilitas, kepercayaan publik, serta penguatan tata kelola perusahaan yang lebih akuntabel.

Berdasarkan analisis tersebut, *Data Protection Compliance Audit* memiliki potensi untuk menjadi instrumen preventif yang mendukung efektivitas implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penerapan audit secara berkala tidak hanya memperkuat kepatuhan hukum, tetapi juga menciptakan sistem pelindungan data yang lebih adaptif terhadap perkembangan teknologi dan risiko keamanan informasi. Oleh karena itu, penguatan mekanisme audit kepatuhan menjadi langkah strategis dalam mewujudkan pelindungan data pribadi yang efektif sekaligus meningkatkan kepastian hukum bagi konsumen dalam transaksi digital.

4. Optimalisasi Kepastian Hukum melalui *Data Protection Compliance Audit*

Kepastian hukum dalam pelindungan data pribadi tidak hanya ditentukan oleh keberadaan peraturan perundang-undangan, tetapi juga oleh efektivitas implementasi dan pengawasannya. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan landasan hukum yang jelas, pelaksanaannya masih memerlukan mekanisme yang mampu memastikan setiap penyelenggara sistem elektronik menjalankan kewajibannya secara konsisten (Indonesia, 2022; Firdaus, 2024). Oleh karena itu, penguatan *Data Protection Compliance Audit* menjadi salah satu upaya strategis untuk meningkatkan efektivitas implementasi pelindungan data pribadi di Indonesia. Dalam konteks tersebut, audit kepatuhan tidak hanya berfungsi untuk menemukan ketidaksesuaian, tetapi juga menyediakan proses evaluasi dan dokumentasi yang dapat menunjukkan tingkat kepatuhan penyelenggara terhadap kewajiban hukum pelindungan data.

Optimalisasi audit kepatuhan dapat dilakukan melalui penyusunan standar audit yang terintegrasi, pelaksanaan evaluasi secara berkala, serta penguatan fungsi pengawasan oleh lembaga yang berwenang. Selain itu, penyelenggara sistem elektronik perlu membangun tata kelola pelindungan data yang didukung oleh kebijakan internal, peningkatan kapasitas sumber daya manusia, serta penerapan sistem keamanan informasi yang memadai. Langkah tersebut tidak hanya bertujuan untuk memenuhi kewajiban hukum, tetapi juga membangun budaya kepatuhan dalam pengelolaan data pribadi. Standar tersebut perlu memuat indikator pemeriksaan yang sekurang-kurangnya mencakup kepatuhan terhadap dasar pemrosesan data, transparansi informasi, pemenuhan hak subjek data, keamanan data, pengelolaan risiko, serta dokumentasi dan tindak lanjut hasil evaluasi (Indonesia, 2022; *International Organization for Standardization*, 2022).

Penerapan *Data Protection Compliance Audit* secara berkelanjutan memberikan manfaat bagi seluruh pihak yang terlibat dalam ekosistem digital. Bagi konsumen, audit kepatuhan meningkatkan jaminan atas keamanan dan kerahasiaan data pribadi sehingga kepercayaan terhadap layanan digital semakin meningkat (Mansawan et al., 2025; Wirayoga & Wisanjaya, 2024). Bagi penyelenggara sistem elektronik, audit menjadi sarana evaluasi untuk memperbaiki kelemahan sistem sekaligus meminimalkan potensi pelanggaran yang dapat menimbulkan sanksi maupun kerugian reputasi (*International Organization for Standardization*, 2022). Dengan adanya evaluasi dan tindak lanjut tersebut, kepatuhan tidak hanya diposisikan sebagai kewajiban normatif, tetapi sebagai proses yang dapat dibuktikan melalui dokumentasi hasil audit dan perbaikan yang dilakukan oleh penyelenggara sistem elektronik.

Berdasarkan hasil analisis, penguatan *Data Protection Compliance Audit* dapat menjadi instrumen preventif untuk memperkuat kepastian hukum dalam pelindungan data pribadi konsumen (Indonesia, 2022; Aristanto et al., 2025; Nugraha & Nasyuha, 2024). Mekanisme tersebut menghubungkan kewajiban hukum dengan proses identifikasi ketidakpatuhan, perbaikan, dan verifikasi secara berkala sehingga risiko pelanggaran dapat ditangani sebelum menimbulkan kerugian bagi konsumen. Bagi pemerintah dan regulator, hasil penelitian ini dapat menjadi bahan pertimbangan dalam memperkuat pedoman pengawasan dan mekanisme evaluasi kepatuhan pelindungan data pribadi. Bagi penyelenggara sistem elektronik, audit kepatuhan dapat digunakan sebagai instrumen untuk mengevaluasi pengelolaan data, memperbaiki ketidakpatuhan, dan mendokumentasikan pemenuhan kewajiban hukum. Dengan demikian, audit kepatuhan tidak hanya berfungsi sebagai instrumen pengawasan, tetapi juga sebagai mekanisme pembuktian dan perbaikan kepatuhan yang mendukung penerapan Undang-Undang Nomor 27 Tahun 2022 secara lebih konsisten dalam transaksi digital.

KESIMPULAN

Berdasarkan hasil penelitian, implementasi pelindungan data pribadi konsumen dalam transaksi digital di Indonesia masih menghadapi tantangan dalam aspek kepatuhan dan pengawasan meskipun telah didukung oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penelitian ini menunjukkan bahwa penguatan *Data Protection Compliance Audit* dapat menjadi instrumen preventif untuk menghubungkan kewajiban hukum berdasarkan UU PDP dengan evaluasi keamanan informasi dan pengelolaan risiko sebagai upaya memperkuat kepastian hukum dalam transaksi digital. Penerapan mekanisme tersebut dapat membantu penyelenggara sistem elektronik mengevaluasi dan memperbaiki pengelolaan data pribadi, sekaligus mendukung pemerintah dan regulator dalam memperkuat pengawasan kepatuhan. Dengan demikian, *Data Protection Compliance Audit* dapat menjadi instrumen pendukung untuk meningkatkan kepatuhan, akuntabilitas, dan kepastian hukum dalam perlindungan data pribadi komsumen.

REFERENSI

Aristianto, E., Hilman, M. H., & Yazid, S. (2025). Evaluating ISO standards for Indonesian PDP Law compliance: A regulatory mapping and literature review. *Scientific Journal of Informatics, 12*(1), 145–158. https://doi.org/10.15294/sji.v12i1.21538

Firdaus, F. H. (2024). Perlindungan dan kepastian hukum bagi pengendali data pribadi di masa depan. *Masalah-Masalah Hukum, 53*(2), 135–144. https://doi.org/10.14710/mmh.53.2.2024.135-144

Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.*

International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements.*

Mansawan, I. S. K., Sassan, J., & Bernard, J. (2025). Legal protection of e-commerce consumers' personal data under Indonesian law. *Jurnal Ilmu Hukum Kyadiren, 7*(1), 538–554. https://doi.org/10.46924/jihk.v7i1.320

Nugraha, A. A., & Nasyuha, A. H. (2024). Integrating ISO 27001 and Indonesia's personal data protection law for data protection requirement model. *Journal of Information Systems and Informatics, 6*(2), 1052–1069. https://doi.org/10.51519/journalisi.v6i2.754

Wirayoga, I. G. P. S., & Wisanjaya, I. G. P. E. (2024). Perlindungan hukum terhadap data pribadi dalam perspektif perlindungan data konsumen e-commerce di Indonesia. *Kertha Semaya: Journal Ilmu Hukum, 12*(8), 1804–1815. https://doi.org/10.24843/KS.2024.v12.i08.p10