Perspektif Administrasi Publik dan hukum
Volume 2, Nomor 2, April 2025
e-ISSN: 3063-797X; p-ISSN: 3063-7805, Hal. 158-175
DOI: https://doi.org/10.62383/perspektif.v2i2.248
Available online at: https://ejournal.appisi.or.id/index.php/Perspektif

Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan

Wyanda Kinanti Syauqi Ramadhani[1*], Sidi Ahyar Wiraguna[2]
[1,2]Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul, Indonesia

Alamat: Jl. Arjuna Utara No.9, Kebon Jeruk, Jakarta 11510
*Korespondensi penulis: wyandakinanti009@gmail.com**

Abstract. *The implementation of personal data protection in information systems at financial services companies is an important issue in this digital era. This study aims to analyze the implementation of personal data protection in information systems at financial services companies in Indonesia after the enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). The main focus of the study is to identify the level of company compliance with the principles of personal data protection, the challenges faced in its implementation, and the legal and business implications that arise. The research method used is normative law with a qualitative approach, supported by literature studies and analysis of related documents. The results of the study show that although the PDP Law has been enacted, the implementation of personal data protection in the information systems of financial services companies still faces various challenges, including system complexity, varying stakeholder awareness, and the need for significant technology investment. This study concludes that more comprehensive efforts are needed from all relevant parties to ensure the effective implementation of the PDP Law and provide concrete suggestions for future improvements.*

Keywords: *Financial Services Companies, Implementation, Information Systems, PDP Law, Personal Data Protection.*

Abstrak. Implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan menjadi isu penting dalam era digital ini. Penelitian ini bertujuan untuk menganalisis implementasi pelindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan di Indonesia pasca pemberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Fokus utama penelitian adalah mengidentifikasi tingkat kepatuhan perusahaan terhadap prinsip-prinsip pelindungan data pribadi, tantangan yang dihadapi dalam implementasinya, serta implikasi hukum dan bisnis yang timbul. Metode penelitian yang digunakan adalah hukum normatif dengan pendekatan kualitatif, didukung oleh studi literatur dan analisis dokumen terkait. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah berlaku, implementasi pelindungan data pribadi dalam sistem informasi perusahaan jasa keuangan masih menghadapi berbagai tantangan, termasuk kompleksitas sistem, kesadaran pemangku kepentingan yang bervariasi, dan kebutuhan investasi teknologi yang signifikan. Penelitian ini menyimpulkan bahwa diperlukan upaya yang lebih komprehensif dari seluruh pihak terkait untuk memastikan implementasi UU PDP yang efektif dan memberikan saran konkret untuk perbaikan di masa depan.

Kata kunci: Perusahaan Jasa Keuangan, Implementasi, Sistem Informasi, UU PDP, Perlindungan Data Pribadi.

1. LATAR BELAKANG

Di era digital yang serba terhubung, data pribadi telah menjadi aset yang sangat berharga, sekaligus rentan terhadap berbagai risiko penyalahgunaan dan kebocoran. Sektor jasa keuangan, sebagai industri yang mengelola informasi finansial dan data pribadi konsumen dalam skala masif, menempati posisi krusial dalam ekosistem pelindungan data. Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai "setiap data tentang seseorang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik [1] atau

Received: Maret 18,, 2025; Revised: Maret 31, 2025; Accepted: April 24, 2025; Published: April 26, 2025

nonelektronik." Karakteristik data yang dikelola oleh perusahaan jasa keuangan seringkali bersifat sensitif, seperti informasi keuangan, riwayat transaksi, data identifikasi pribadi, yang jika jatuh ke tangan yang salah dapat menimbulkan kerugian finansial dan non-finansial yang signifikan bagi individu.

Urgensi pelindungan data pribadi tidak hanya terletak pada aspek keamanan dan kerugian materiil, tetapi juga pada hak asasi manusia, khususnya hak atas privasi dan kebebasan informasi. Perkembangan teknologi informasi yang pesat, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, telah membawa kemudahan dalam pengelolaan dan pemrosesan data, namun juga meningkatkan potensi risiko pelanggaran privasi. Perusahaan jasa keuangan, dengan sistem informasi yang kompleks dan terintegrasi, memiliki tanggung jawab besar untuk memastikan keamanan dan kerahasiaan data pribadi yang mereka kelola sesuai dengan amanat peraturan perundang-undangan. Kegagalan dalam melindungi data pribadi tidak hanya berpotensi melanggar ketentuan UU PDP, namun juga dapat merusak reputasi perusahaan dan kepercayaan konsumen, yang pada akhirnya dapat berdampak negatif terhadap keberlangsungan bisnis.

Urgensi dan Signifikansi Pelindungan Data Pribadi di Era Digital dalam Konteks Perusahaan Jasa Keuangan

Di era digital yang ditandai dengan eksponensi data dan konektivitas tanpa batas, data pribadi menjelma menjadi komoditas krusial yang menyimpan nilai ekonomi dan informasi yang substansial. Sektor jasa keuangan, sebagai garda terdepan dalam mengelola aset dan transaksi finansial masyarakat, memiliki tanggung jawab yang unik dan mendesak terkait pelindungan data pribadi. Perusahaan-perusahaan dalam industri ini tidak hanya menyimpan data identitas dasar, tetapi juga informasi finansial yang sensitif, riwayat transaksi, skor kredit, dan preferensi investasi. Volume dan sensitivitas data yang dikelola menjadikan perusahaan jasa keuangan sebagai target utama serangan siber dan potensi penyalahgunaan data.

Menurut studi dari IBM Security (2023 Cost of a Data Breach Report), sektor keuangan secara konsisten menduduki peringkat teratas dalam biaya rata-rata kebocoran data, yang menggarisbawahi kerugian finansial dan reputasi yang signifikan akibat insiden keamanan siber. Lebih lanjut, Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 secara implisit mengakui hak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, serta hak atas rasa aman dan perlindungan dari ancaman ketakutan. [1] Dalam konteks digital, hak ini diejawantahkan dalam pelindungan data pribadi.

Menurut laporan "The Global Risks Report 2024" dari World Economic Forum, risiko siber dan disinformasi menjadi ancaman global yang semakin nyata, menggarisbawahi kerentanan infrastruktur digital dan data pribadi. Bagi perusahaan jasa keuangan, kebocoran data tidak hanya berpotensi mengakibatkan kerugian finansial langsung bagi konsumen dan perusahaan, tetapi juga merusak reputasi yang dibangun bertahun-tahun, mengikis kepercayaan pelanggan, dan bahkan mengancam stabilitas sistem keuangan secara keseluruhan. Pasal 28G UUD 1945, yang menjamin hak atas perlindungan diri pribadi dan rasa aman, mendapatkan relevansi yang lebih mendalam di era digital ini, menuntut negara dan entitas swasta, termasuk perusahaan jasa keuangan, untuk memastikan pelindungan data pribadi warga negara. Kegagalan dalam melindungi data pribadi di sektor jasa keuangan dapat berakibat fatal, tidak hanya bagi individu yang datanya disalahgunakan (misalnya, penipuan finansial, pencurian identitas), tetapi juga bagi stabilitas sistem keuangan secara keseluruhan. Kehilangan kepercayaan publik terhadap institusi keuangan akibat kebocoran data dapat memicu penarikan dana massal dan mengganggu likuiditas pasar. Oleh karena itu, implementasi pelindungan data pribadi yang efektif bukan hanya sekadar kepatuhan terhadap regulasi, tetapi juga merupakan imperatif bisnis dan etika bagi perusahaan jasa keuangan. Perusahaan jasa keuangan seringkali beroperasi di berbagai yurisdiksi dengan regulasi pelindungan data yang berbeda-beda. Ketidakseragaman ini menciptakan tantangan dalam memastikan kepatuhan lintas batas dan melindungi data warga negara Indonesia yang diproses di luar negeri, serta data warga negara asing yang diproses di Indonesia. UU PDP hadir sebagai upaya untuk menyelaraskan standar pelindungan data di Indonesia dengan praktik internasional terbaik, sekaligus memberikan kedaulatan atas data pribadi warga negara.

Latar Belakang Lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai Respons terhadap Kebutuhan Perlindungan yang Lebih Kuat dan Komprehensif

Sebelum diundangkannya UU PDP Nomor 27 Tahun 2022, lanskap hukum pelindungan data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral dan tidak memiliki kerangka kerja yang komprehensif. Beberapa ketentuan terkait pelindungan data dapat ditemukan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, serta peraturan sektoral seperti Peraturan Bank Indonesia (PBI) terkait kerahasiaan data nasabah bank. Namun, peraturan-peraturan ini seringkali bersifat parsial dan tidak secara eksplisit mengatur prinsip-prinsip pelindungan data

pribadi secara menyeluruh, hak-hak subjek data, maupun kewajiban pengendali dan prosesor data.

Kebutuhan akan undang-undang pelindungan data pribadi yang lebih kuat dan komprehensif semakin mendesak seiring dengan perkembangan ekonomi digital dan meningkatnya insiden kebocoran data. Regulasi yang kuat diharapkan dapat menciptakan kepastian hukum, meningkatkan akuntabilitas pengendali data, dan memberdayakan individu sebagai subjek data. UU PDP hadir sebagai respons terhadap kebutuhan ini, mengadopsi prinsip-prinsip pelindungan data yang diakui secara internasional, seperti yang tercantum dalam General Data Protection Regulation (GDPR) Uni Eropa, meskipun dengan karakteristik dan penyesuaian terhadap konteks hukum dan sosial Indonesia.Sebelum pengesahan UU PDP Nomor 27 Tahun 2022, kerangka hukum pelindungan data pribadi di Indonesia dapat diibaratkan sebagai mozaik yang terdiri dari berbagai peraturan sektoral dengan cakupan yang terbatas. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya memang mengatur beberapa aspek terkait data elektronik, namun fokus utamanya bukanlah pelindungan data pribadi secara komprehensif. Peraturan sektoral seperti Peraturan Bank Indonesia (PBI) dan peraturan Otoritas Jasa Keuangan (OJK) menyentuh aspek kerahasiaan data nasabah, namun belum mengadopsi prinsip-prinsip pelindungan data yang holistik seperti yang diakui secara internasional.

Kesenjangan hukum ini semakin terasa mendesak seiring dengan pesatnya perkembangan ekonomi digital, masifnya pengumpulan dan pemrosesan data pribadi oleh berbagai entitas, serta meningkatnya frekuensi dan skala insiden kebocoran data. Kasus-kasus penyalahgunaan data pribadi yang terjadi sebelum lahirnya UU PDP menunjukkan betapa rentannya individu tanpa adanya payung hukum yang kuat untuk melindungi hak-hak mereka. Tuntutan masyarakat sipil, akademisi, dan komunitas internasional akan regulasi pelindungan data yang lebih kuat menjadi katalisator utama dalam proses legislasi UU PDP. UU PDP tidak hanya bertujuan untuk mengisi kekosongan hukum, tetapi juga untuk mengadopsi standar pelindungan data yang sejalan dengan praktik terbaik global, seperti yang tercermin dalam General Data Protection Regulation (GDPR) Uni Eropa. Dengan menetapkan definisi yang jelas mengenai data pribadi, mengatur secara rinci prinsip-prinsip pemrosesan data, memberikan hak-hak yang kuat kepada subjek data, dan memberlakukan kewajiban yang signifikan kepada pengendali dan prosesor data, UU PDP menandai perubahan paradigma dalam tata kelola data pribadi di Indonesia. Kehadirannya diharapkan dapat menciptakan kepastian hukum, meningkatkan akuntabilitas entitas yang memproses data, dan memberdayakan individu untuk memiliki kontrol yang lebih besar atas data pribadi mereka.UU

PDP secara fundamental mengubah lanskap pelindungan data pribadi di Indonesia dengan menetapkan definisi yang jelas mengenai data pribadi, mengatur prinsip-prinsip pemrosesan data, memberikan hak-hak kepada individu sebagai subjek data, dan memberlakukan kewajiban yang signifikan kepada pengendali dan prosesor data. Kehadiran UU PDP menandai era baru dalam tata kelola data pribadi di Indonesia, termasuk dalam sektor jasa keuangan yang memiliki karakteristik pengelolaan data yang unik dan kompleks.

Identifikasi Permasalahan Terkait Implementasi UU PDP dalam Sistem Informasi Perusahaan Jasa Keuangan, Termasuk Potensi Risiko Kebocoran Data, Tantangan Teknis, dan Interpretasi Ketentuan Hukum

Meskipun UU PDP merupakan langkah maju yang signifikan, implementasinya dalam sistem informasi perusahaan jasa keuangan tidak terlepas dari berbagai permasalahan dan tantangan. Sistem informasi yang digunakan oleh perusahaan jasa keuangan seringkali merupakan hasil dari evolusi teknologi selama bertahun-tahun, yang melibatkan integrasi berbagai platform, aplikasi, dan database yang mungkin tidak dirancang dengan mempertimbangkan prinsip-prinsip pelindungan data modern. Migrasi dan adaptasi sistem-sistem ini agar sesuai dengan ketentuan UU PDP memerlukan perencanaan yang matang, sumber daya yang besar, dan keahlian teknis yang mendalam. Potensi risiko kebocoran data menjadi perhatian utama dalam konteks perusahaan jasa keuangan. Insiden keamanan siber, baik yang disebabkan oleh serangan eksternal maupun kelalaian internal, dapat mengakibatkan kerugian finansial yang besar, gangguan operasional, dan kerusakan reputasi yang sulit dipulihkan. UU PDP Pasal 46 secara tegas mengatur kewajiban pemberitahuan insiden kebocoran data kepada subjek data dan Otoritas Pelindungan Data Pribadi (ODP), yang menuntut perusahaan untuk memiliki mekanisme deteksi, respons, dan notifikasi yang efektif. Selain tantangan teknis, interpretasi terhadap berbagai ketentuan dalam UU PDP juga menimbulkan permasalahan tersendiri. Konsep-konsep seperti "kepentingan yang sah" (Pasal 6 huruf f), penentuan kapan persetujuan dianggap sah (Pasal 7), dan bagaimana menerapkan prinsip minimisasi data dalam layanan keuangan yang kompleks memerlukan analisis hukum yang mendalam dan berpotensi menimbulkan ketidakseragaman dalam implementasi di berbagai perusahaan. Ketiadaan pedoman implementasi yang spesifik untuk sektor jasa keuangan dari ODP pada tahap awal implementasi UU PDP dapat memperburuk ketidakpastian ini. Aspek organisasi dan tata kelola data menjadi krusial dalam implementasi UU PDP. Penunjukan DPO yang memiliki pemahaman mendalam tentang hukum pelindungan data dan teknologi informasi (Pasal 53), penyusunan kebijakan dan prosedur pelindungan data yang

komprehensif, serta integrasi prinsip-prinsip pelindungan data ke dalam seluruh siklus hidup pengembangan sistem informasi (*Security and Privacy by Design*) memerlukan perubahan budaya dan komitmen dari seluruh organisasi. Penelitian ini bertujuan untuk menganalisis secara komprehensif tantangan-tantangan ini dan mengidentifikasi strategi serta praktik terbaik dalam mengimplementasikan pelindungan data pribadi dalam sistem informasi perusahaan jasa keuangan di Indonesia pasca pemberlakuan UU PDP, dengan harapan dapat memberikan kontribusi bagi terciptanya ekosistem keuangan digital yang aman dan terpercaya.Kesadaran dan pemahaman mengenai UU PDP di kalangan karyawan perusahaan jasa keuangan juga menjadi faktor krusial. Pelanggaran terhadap ketentuan pelindungan data seringkali disebabkan oleh human error atau kurangnya pemahaman mengenai kebijakan dan prosedur yang berlaku. Oleh karena itu, program pelatihan dan peningkatan kesadaran yang berkelanjutan menjadi esensial untuk memastikan kepatuhan terhadap UU PDP di seluruh organisasi. Penelitian ini bertujuan untuk menganalisis secara mendalam tantangan-tantangan ini dan mengidentifikasi praktik-praktik terbaik dalam implementasi pelindungan data pribadi dalam sistem informasi perusahaan jasa keuangan pasca pemberlakuan UU PDP.

2. METODE PENELITIAN

Studi kasus dengan pendekatan kualitatif untuk menganalisis implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan.

Analisis data sekunder dari dokumen perusahaan dan sumber lain yang relevan untuk memperoleh informasi tentang implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan.

Langkah-Langkah Penelitian

Pengumpulan Data : Data yang digunakan dalam penelitian ini adalah data primer yang diperoleh dari wawancara dengan pihak perusahaan jasa keuangan dan data sekunder yang diperoleh dari dokumen perusahaan.

Analisis Data: Data yang diperoleh akan dianalisis menggunakan metode analisis kualitatif untuk memperoleh pemahaman yang lebih dalam tentang implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan.

Pengujian Validitas: Validitas data akan diuji menggunakan metode triangulasi untuk memastikan bahwa data yang diperoleh akurat dan dapat dipercaya.

Tujuan Penelitian

Penelitian ini bertujuan untuk: Menganalisis Implementasi Perlindungan Data Pribadi : Penelitian ini bertujuan untuk menganalisis implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan. Mengevaluasi Efektivitas: Penelitian ini bertujuan untuk mengevaluasi efektivitas implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan. Mengidentifikasi Kelemahan dan Tantangan : Penelitian ini bertujuan untuk mengidentifikasi kelemahan dan tantangan yang dihadapi dalam implementasi perlindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan.

Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi:

- Perusahaan Jasa Keuangan: Penelitian ini diharapkan dapat memberikan informasi yang berguna bagi perusahaan jasa keuangan dalam meningkatkan implementasi perlindungan data pribadi dalam sistem informasi.
- Regulator: Penelitian ini diharapkan dapat memberikan informasi yang berguna bagi regulator dalam mengembangkan peraturan yang lebih efektif untuk melindungi data pribadi nasabah.
- Akademisi: Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu hukum, khususnya dalam bidang hukum pelindungan data pribadi dan hukum teknologi informasi, serta menjadi referensi bagi penelitian selanjutnya.
- Praktisi: Hasil penelitian ini diharapkan dapat memberikan masukan yang berguna bagi perusahaan jasa keuangan, regulator, dan pemangku kepentingan lainnya dalam meningkatkan implementasi pelindungan data pribadi sesuai dengan ketentuan UU PDP.

Rumusan Masalah

- Bagaimana implementasi ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) diterapkan dalam sistem informasi pada perusahaan jasa keuangan di Indonesia?
- Apa saja tantangan dan hambatan yang dihadapi perusahaan jasa keuangan dalam mengimplementasikan pelindungan data pribadi sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022?

3. HASIL DAN PEMBAHASAN

Implementasi ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dalam sistem informasi perusahaan jasa keuangan merupakan proses yang kompleks dan melibatkan berbagai aspek. Pasal 5 UU PDP secara eksplisit mengatur prinsip-prinsip pelindungan data pribadi yang wajib dipatuhi oleh setiap pengendali data pribadi, termasuk perusahaan jasa keuangan. Prinsip-prinsip tersebut meliputi prinsip akuntabilitas, prinsip kehati-hatian, prinsip kerahasiaan, prinsip pembatasan tujuan, prinsip minimisasi data, prinsip pembatasan penyimpanan, prinsip integritas dan kerahasiaan, serta prinsip pertanggungjawaban. Dalam konteks sistem informasi, implementasi prinsip-prinsip ini memerlukan adopsi kebijakan, prosedur, dan teknologi yang tepat.

Salah satu aspek penting dalam implementasi adalah pemenuhan hak-hak subjek data pribadi sebagaimana diatur dalam Pasal 4 hingga Pasal 15 UU PDP. Perusahaan jasa keuangan harus memastikan bahwa sistem informasi mereka mampu memfasilitasi hak subjek data, seperti hak untuk mengakses, memperbaiki, menghapus, menarik kembali persetujuan, dan mengajukan keberatan terhadap pemrosesan data pribadi. Misalnya, sistem harus memiliki mekanisme yang jelas dan mudah diakses bagi konsumen untuk mengajukan permintaan terkait data pribadi mereka. Lebih lanjut, Pasal 20 hingga Pasal 31 UU PDP mengatur mengenai kewajiban pengendali data pribadi, termasuk kewajiban untuk menerapkan langkah-langkah teknis dan organisatoris yang tepat guna melindungi data pribadi dari akses yang tidak sah, pengungkapan, modifikasi, atau penghancuran. Ini berarti perusahaan jasa keuangan perlu menginvestasikan sumber daya dalam sistem keamanan informasi, seperti enkripsi data, firewall, sistem deteksi intrusi, dan audit keamanan berkala.

Implementasi pelindungan data pribadi dalam sistem informasi tidak hanya terbatas pada aspek teknis, tetapi juga memerlukan kerangka kerja tata kelola data yang kuat. Ini mencakup penunjukan petugas pelindungan data (Data Protection Officer - DPO) sebagaimana diamanatkan dalam Pasal 53 UU PDP bagi pengendali data yang memenuhi kriteria tertentu, serta penyusunan kebijakan privasi yang transparan dan mudah dipahami oleh konsumen. Lebih lanjut, Pasal 32 hingga Pasal 37 UU PDP mengatur mengenai prosesor data pribadi, yang seringkali terlibat dalam operasional sistem informasi perusahaan jasa keuangan. Pengendali data (perusahaan jasa keuangan) memiliki kewajiban untuk memastikan bahwa prosesor data juga mematuhi ketentuan UU PDP dan memiliki standar keamanan yang memadai.

Selain itu, implementasi UU PDP dalam sistem informasi perusahaan jasa keuangan juga terkait erat dengan peraturan perundang-undangan lain yang relevan, seperti Peraturan Bank Indonesia (PBI) terkait dengan keamanan sistem informasi perbankan dan perlindungan

konsumen. Sinergi antara UU PDP dan peraturan sektoral ini menjadi krusial untuk menciptakan ekosistem pelindungan data yang holistik. Tantangan seringkali muncul dalam mengintegrasikan berbagai regulasi ini ke dalam sistem informasi yang sudah ada, serta memastikan kepatuhan yang berkelanjutan seiring dengan perkembangan teknologi dan ancaman keamanan siber yang semakin canggih.

Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dalam sistem informasi perusahaan jasa keuangan di Indonesia merupakan transformasi multidimensional yang menyentuh aspek hukum, teknologi, dan operasional.

Pasal 5 UU PDP menggariskan prinsip-prinsip fundamental yang harus diinternalisasikan dalam setiap proses permutasen data pribadi, termasuk dalam arsitektur dan operasional sistem informasi. Prinsip-prinsip seperti akuntabilitas, kehati-hatian, kerahasiaan, pembatasan tujuan, minimisasi data, pembatasan penyimpanan, integritas dan kerahasiaan, serta pertanggungjawaban, menuntut perusahaan jasa keuangan untuk mendesain sistem informasi mereka dengan mempertimbangkan siklus hidup data secara holistik, mulai dari pengumpulan hingga penghapusan.

Salah satu manifestasi implementasi prinsip-prinsip ini dalam sistem informasi adalah adopsi mekanisme *privacy by design* dan *privacy by default*. *Privacy by design* mengamanatkan bahwa pertimbangan pelindungan data pribadi harus diintegrasikan sejak tahap perancangan dan pengembangan sistem informasi, bukan sebagai fitur tambahan di kemudian hari.

Sementara itu, *privacy by default* berarti bahwa pengaturan privasi yang paling ketat harus menjadi konfigurasi awal sistem, dan pengguna harus secara aktif memberikan persetujuan untuk opsi yang kurang pribadi (privat). Penerapan kedua konsep ini memerlukan perubahan mendasar dalam siklus pengembangan perangkat lunak dan infrastruktur teknologi informasi perusahaan jasa keuangan.

Pemenuhan hak-hak subjek data pribadi, sebagaimana diatur dalam Pasal 4 hingga Pasal 15 UU PDP, juga memiliki implikasi signifikan terhadap desain dan fungsionalitas sistem informasi.

Perusahaan harus menyediakan mekanisme yang mudah diakses dan responsif bagi konsumen untuk melaksanakan hak mereka, seperti hak akses (meminta informasi mengenai pemrosesan data), hak koreksi (memperbaiki data yang tidak akurat), hak penghapusan (menghapus data dalam kondisi tertentu), hak pembatasan pemrosesan, hak portabilitas data (mentransfer data ke pengendali lain), dan hak untuk mengajukan keberatan. Sistem informasi harus mampu mengelola permintaan-permintaan ini secara efisien dan aman, serta mencatat setiap interaksi terkait data pribadi.

Kewajiban pengendali data pribadi, yang diatur dalam Pasal 20 hingga Pasal 31 UU PDP, menuntut perusahaan jasa keuangan untuk mengimplementasikan langkah-langkah teknis dan organisatoris yang memadai untuk menjamin keamanan data pribadi. Ini mencakup implementasi kebijakan keamanan informasi yang komprehensif, penggunaan teknologi enkripsi (baik *at rest* maupun *in transit*), penerapan kontrol akses yang ketat berdasarkan prinsip *least privilege*, audit keamanan berkala, dan manajemen kerentanan sistem. Menurut standar ISO 27001 tentang Sistem Manajemen Keamanan Informasi, perusahaan perlu mengadopsi pendekatan berbasis risiko untuk mengidentifikasi aset informasi, menilai ancaman dan kerentanan, serta menerapkan kontrol keamanan yang proporsional.

Penunjukan Data Protection Officer (DPO), sebagaimana diamanatkan dalam Pasal 53 UU PDP bagi pengendali data dengan skala besar atau pemrosesan data yang berisiko tinggi, juga berimplikasi pada struktur organisasi dan sistem informasi. DPO berperan sebagai penghubung antara perusahaan, subjek data, dan ODP, serta bertanggung jawab untuk memantau kepatuhan terhadap UU PDP. Sistem informasi harus mendukung fungsi DPO dalam melaksanakan tugasnya, seperti menyediakan akses ke informasi pemrosesan data dan memfasilitasi komunikasi dengan subjek data.

Integrasi dengan peraturan sektoral, seperti PBI terkait keamanan sistem informasi perbankan, juga menjadi aspek penting dalam implementasi UU PDP. Perusahaan jasa keuangan harus memastikan bahwa sistem informasi mereka tidak hanya mematuhi UU PDP, tetapi juga regulasi lain yang relevan. Harmonisasi antara berbagai peraturan ini memerlukan pemahaman yang mendalam mengenai persyaratan hukum yang berbeda dan kemampuan untuk mengimplementasikan kontrol yang memenuhi berbagai standar.

Prinsip kehati-hatian dan kerahasiaan secara langsung berimplikasi pada arsitektur keamanan sistem informasi. Perusahaan jasa keuangan harus mengadopsi lapisan keamanan berlapis (*defense in depth*), termasuk firewall, sistem deteksi intrusi dan pencegahan (IDPS), segmentasi jaringan, dan kontrol akses berbasis peran (*role-based access control*). Enkripsi data, baik saat disimpan (*at rest*) maupun saat ditransmisikan (*in transit*) menggunakan protokol yang kuat (misalnya TLS 1.3), menjadi krusial untuk menjaga kerahasiaan data, sebagaimana diamanatkan secara implisit dalam prinsip kerahasiaan dan integritas (Pasal 5 huruf g). Implementasi ini memerlukan pemilihan algoritma enkripsi yang teruji dan pengelolaan kunci enkripsi yang aman. Prinsip pembatasan tujuan dan minimisasi data menuntut perusahaan untuk mendesain sistem informasi yang hanya mengumpulkan dan

memproses data yang relevan dan proporsional dengan tujuan yang telah ditetapkan dan disetujui.

Sistem harus memiliki mekanisme untuk membatasi input data yang tidak perlu dan secara otomatis menghapus atau menganonimkan data yang tidak lagi relevan setelah periode retensi yang ditentukan. Implementasi ini dapat melibatkan desain formulir pengumpulan data yang selektif dan kebijakan retensi data yang jelas dan terotomatisasi dalam sistem.

Prinsip pembatasan penyimpanan dan prinsip pertanggungjawaban menyoroti pentingnya siklus hidup data dalam sistem informasi. Perusahaan harus memiliki kebijakan dan mekanisme teknis

untuk memastikan data hanya disimpan selama diperlukan dan dimusnahkan secara aman setelahnya. Sistem harus memiliki fitur untuk melacak masa retensi data dan melakukan penghapusan data secara permanen (*data wiping*) atau anonimisasi yang tidak dapat dikembalikan (*irreversible anonymization*).

Prinsip pertanggungjawaban menuntut perusahaan untuk dapat menunjukkan kepatuhan terhadap seluruh prinsip UU PDP, yang berarti sistem informasi harus mampu menghasilkan laporan dan log yang relevan untuk keperluan audit dan akuntabilitas.

Pemenuhan hak-hak subjek data (Pasal 4-15 UU PDP) memerlukan perancangan antarmuka pengguna (user interface) dan alur kerja (workflow) dalam sistem informasi yang memungkinkan konsumen untuk dengan mudah mengajukan permintaan terkait hak mereka. Misalnya, sistem harus menyediakan portal atau mekanisme daring yang aman bagi konsumen untuk mengakses data pribadi mereka, mengajukan koreksi jika ada kesalahan, meminta penghapusan data dalam kondisi yang diizinkan, menarik kembali persetujuan, atau mengajukan keberatan terhadap pemrosesan data untuk tujuan tertentu. Sistem juga harus mencatat dan mengelola setiap permintaan ini secara efisien dan sesuai dengan jangka waktu yang ditentukan oleh UU PDP. Implementasi hak portabilitas data (Pasal 14) memerlukan sistem yang mampu mengekspor data dalam format yang terstruktur dan umum digunakan agar dapat ditransfer ke pengendali data lain. Implementasi pelindungan data pribadi sesuai dengan ketentuan UU PDP dalam sistem informasi perusahaan jasa keuangan di Indonesia dihadapkan pada serangkaian tantangan dan hambatan yang kompleks. Salah satu tantangan fundamental adalah warisan sistem (legacy systems) yang masih banyak digunakan oleh perusahaan jasa keuangan.

Sistem-sistem ini seringkali dibangun sebelum adanya kesadaran yang kuat mengenai pentingnya pelindungan data dan mungkin tidak memiliki arsitektur yang sesuai dengan prinsip-prinsip UU PDP. Memodifikasi atau mengganti sistem-sistem ini memerlukan investasi

waktu, biaya, dan sumber daya yang signifikan, serta berpotensi mengganggu operasional bisnis.

Kurangnya pemahaman dan kesadaran yang komprehensif mengenai UU PDP di seluruh tingkatan organisasi merupakan hambatan lain yang signifikan. Kepatuhan terhadap UU PDP bukan hanya tanggung jawab departemen hukum atau TI, tetapi memerlukan pemahaman dan komitmen dari seluruh karyawan yang berinteraksi dengan data pribadi. Program pelatihan dan sosialisasi yang efektif sangat penting untuk mengatasi hambatan ini, namun implementasinya secara merata dan berkelanjutan dapat menjadi tantangan tersendiri.Investasi teknologi yang diperlukan untuk memenuhi persyaratan UU PDP juga menjadi kendala, terutama bagi perusahaan jasa keuangan skala kecil dan menengah. Implementasi solusi keamanan canggih, sistem manajemen persetujuan (*consent management platforms*), solusi anonimisasi dan pseudonimisasi data, serta sistem untuk merespons permintaan hak subjek data memerlukan alokasi anggaran yang substansial. Pasal 47 UU PDP mengatur mengenai kewajiban untuk mencatat kegiatan pemrosesan data pribadi, yang memerlukan implementasi sistem audit log yang komprehensif dan aman.

Tantangan dalam interpretasi dan implementasi beberapa pasal UU PDP juga menjadi hambatan. Ketidakjelasan mengenai definisi beberapa istilah atau ruang lingkup kewajiban tertentu dapat menyebabkan kebingungan dan inkonsistensi dalam praktik pelindungan data. Misalnya, penentuan "persetujuan yang sah" (informed consent) dalam konteks layanan keuangan yang kompleks memerlukan kehati-hatian agar tidak bersifat manipulatif atau menyesatkan.

Keterlambatan dalam penerbitan peraturan pelaksana oleh ODP dapat memperpanjang ketidakpastian ini. Aspek budaya organisasi juga memainkan peran penting dalam keberhasilan implementasi UU PDP. Perusahaan jasa keuangan perlu menumbuhkan budaya yang menghargai privasi dan keamanan data sebagai prioritas utama. Perubahan budaya memerlukan waktu dan upaya yang konsisten dari kepemimpinan perusahaan untuk menginternalisasi nilai-nilai pelindungan data di seluruh proses bisnis dan pengambilan keputusan.

Lanskap ancaman siber yang terus berkembang menghadirkan tantangan berkelanjutan bagi upaya pelindungan data pribadi. Perusahaan jasa keuangan harus terus-menerus memantau dan memperbarui sistem keamanan mereka untuk menghadapi serangan siber yang semakin canggih dan terarah. Implementasi UU PDP harus berjalan seiring dengan upaya peningkatan ketahanan siber perusahaan untuk memastikan data pribadi tetap aman dari akses yang tidak sah dan kebocoran.

Kurangnya pemahaman dan kesadaran yang mendalam mengenai UU PDP di seluruh lapisan organisasi menjadi hambatan signifikan lainnya. Kepatuhan terhadap UU PDP bukan hanya tanggung jawab departemen TI atau hukum, tetapi memerlukan pemahaman dan internalisasi prinsip-prinsip pelindungan data oleh seluruh karyawan yang berinteraksi dengan data pribadi, mulai dari *front-office* hingga manajemen senior. Mengubah pola pikir dan perilaku terkait pengelolaan data memerlukan program pelatihan yang komprehensif dan berkelanjutan, serta dukungan dari kepemimpinan perusahaan untuk menanamkan budaya sadar privasi (*privacy-aware culture*).

Investasi finansial yang signifikan dalam teknologi dan infrastruktur pelindungan data menjadi hambatan bagi sebagian perusahaan, terutama skala kecil dan menengah. Implementasi solusi keamanan canggih, sistem manajemen persetujuan (*consent management platforms*), solusi anonimisasi dan pseudonimisasi data, serta platform untuk merespons permintaan hak subjek data memerlukan alokasi anggaran yang besar. Perusahaan perlu menimbang biaya investasi dengan potensi risiko dan konsekuensi ketidakpatuhan terhadap UU PDP.

Tantangan dan hambatan dalam mengimplementasikan pelindungan data pribadi sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 (UU PDP) dalam sistem informasi perusahaan jasa keuangan sangat beragam. Salah satu tantangan utama adalah kompleksitas sistem informasi yang dimiliki oleh banyak perusahaan jasa keuangan. Sistem ini seringkali merupakan warisan (legacy system) yang telah ada sejak lama dan terintegrasi dengan berbagai aplikasi dan database yang berbeda. Memastikan kepatuhan terhadap prinsip-prinsip UU PDP, seperti minimisasi data dan pembatasan penyimpanan, dalam sistem yang kompleks ini memerlukan upaya yang signifikan dalam hal audit data, pemetaan proses bisnis, dan modifikasi sistem.

Salah satu hambatan signifikan adalah kurangnya pemahaman dan kesadaran yang merata mengenai UU PDP di kalangan pemangku kepentingan, baik di internal perusahaan (karyawan dari berbagai tingkatan) maupun di kalangan konsumen. Pasal 38 UU PDP mengamanatkan kewajiban bagi pengendali data untuk memberikan informasi yang jelas dan transparan kepada subjek data mengenai pemrosesan data pribadi mereka. Namun, mengkomunikasikan informasi ini secara efektif melalui sistem informasi yang mudah dipahami oleh semua pihak merupakan tantangan tersendiri.

Investasi teknologi yang signifikan juga menjadi hambatan bagi sebagian perusahaan jasa keuangan, terutama skala kecil dan menengah. Implementasi fitur-fitur keamanan yang canggih, sistem manajemen persetujuan (consent management), dan mekanisme respons

terhadap permintaan hak subjek data memerlukan alokasi anggaran yang besar. Pasal 46 UU PDP mengatur mengenai kewajiban pengendali data untuk memberitahukan kepada subjek data dan kepada Otoritas Pelindungan Data Pribadi (ODP) apabila terjadi kegagalan pelindungan data pribadi. Membangun sistem notifikasi yang efektif dan responsif terhadap insiden keamanan siber juga memerlukan infrastruktur teknologi dan sumber daya manusia yang memadai.

Selain itu, interpretasi dan implementasi beberapa ketentuan dalam UU PDP masih menjadi tantangan. Misalnya, penentuan kriteria "kepentingan yang sah" sebagai dasar pemrosesan data pribadi (Pasal 6 huruf f UU PDP) dalam konteks layanan keuangan memerlukan analisis yang cermat agar tidak bertentangan dengan hak-hak subjek data. Ketidakjelasan dalam beberapa aspek hukum ini dapat menimbulkan ketidakpastian bagi perusahaan dalam mengimplementasikan kebijakan dan prosedur yang sesuai.

Diperlukan panduan dan regulasi yang lebih rinci dari ODP untuk mengatasi ambiguitas dalam interpretasi beberapa pasal UU PDP.

Tantangan lintas batas (cross-border data transfer) juga relevan bagi perusahaan jasa keuangan yang memiliki operasional atau transaksi internasional. Pasal 56 UU PDP mengatur mengenai transfer data pribadi ke luar wilayah Negara Kesatuan Republik Indonesia, yang memerlukan kepatuhan terhadap persyaratan tertentu untuk memastikan tingkat pelindungan data yang setara. Mengelola transfer data lintas batas dalam sistem informasi global perusahaan jasa keuangan memerlukan pemahaman yang mendalam terhadap regulasi di berbagai yurisdiksi dan implementasi mekanisme transfer data yang sah dan aman.

Aspek tata kelola data (*data governance*) yang matang juga menjadi prasyarat penting untuk implementasi UU PDP yang efektif. Perusahaan perlu menetapkan kebijakan, prosedur, dan tanggung jawab yang jelas terkait pengumpulan, pemrosesan, penyimpanan, dan penghapusan data pribadi. Implementasi tata kelola data yang kuat memerlukan perubahan dalam struktur organisasi, alokasi sumber daya, dan proses pengambilan keputusan terkait data.

Lanskap ancaman siber yang terus berkembang menghadirkan tantangan berkelanjutan. Perusahaan jasa keuangan harus terus-menerus memantau dan memperbarui sistem keamanan mereka untuk menghadapi serangan siber yang semakin canggih dan terarah. Implementasi UU PDP harus berjalan seiring dengan upaya peningkatan ketahanan siber (*cyber resilience*) perusahaan, termasuk implementasi kerangka kerja keamanan siber seperti NIST Cybersecurity Framework atau ISO 27001, serta pelaksanaan pengujian penetrasi (*penetration testing*) dan audit keamanan berkala.

Selain aspek teknis, hukum, dan operasional yang telah dibahas, implementasi UU PDP dalam sistem informasi perusahaan jasa keuangan di Indonesia dapat dianalisis lebih lanjut melalui perspektif komparatif dengan regulasi serupa di yurisdiksi lain yang lebih maju dalam pelindungan data, seperti General Data Protection Regulation (GDPR) di Uni Eropa atau California Consumer Privacy Act (CCPA) di Amerika Serikat.[1] Perbandingan ini dapat memberikan wawasan berharga mengenai praktik terbaik, tantangan yang mungkin timbul di masa depan, dan potensi evolusi regulasi di Indonesia. Misalnya, GDPR memiliki penekanan yang kuat pada hak untuk dilupakan (*right to be forgotten*) dan denda yang sangat signifikan untuk pelanggaran, yang dapat menjadi pertimbangan bagi penguatan implementasi dan penegakan hukum UU PDP di Indonesia. CCPA, dengan fokusnya pada hak konsumen untuk mengetahui data apa yang dikumpulkan dan hak untuk menolak penjualan data, dapat memberikan inspirasi untuk meningkatkan transparansi dan kontrol konsumen dalam sistem informasi perusahaan jasa keuangan di Indonesia.

4. KESIMPULAN DAN SARAN

Kesimpulan

Transformasi Sistemik dan Imperatif Kepatuhan UU PDP dalam Ekosistem Digital Perusahaan Jasa Keuangan

Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dalam sistem informasi perusahaan jasa keuangan di Indonesia bukan merupakan tugas parsial atau sekadar pemenuhan kewajiban hukum semata, melainkan sebuah transformasi sistemik yang fundamental dalam merespons lanskap digital yang terus berkembang dan tuntutan etis serta hukum yang semakin menguat terkait pelindungan hak-hak individu atas data pribadi mereka.

Analisis mendalam terhadap berbagai aspek implementasi ini secara jelas mengindikasikan bahwa perusahaan jasa keuangan dihadapkan pada imperatif untuk secara proaktif dan komprehensif mengintegrasikan prinsip-prinsip dan ketentuan UU PDP ke dalam inti operasional dan arsitektur teknologi informasi mereka. Proses ini melampaui sekadar adopsi kebijakan dan prosedur formal, menuntut perubahan mendasar dalam cara data dikumpulkan, diproses, disimpan, dan dihapus dalam seluruh siklus hidupnya di dalam sistem informasi perusahaan.

Keberhasilan implementasi UU PDP secara langsung berkorelasi dengan kemampuan perusahaan jasa keuangan untuk membangun dan mempertahankan kepercayaan konsumen, yang merupakan aset paling berharga dalam industri yang sangat bergantung pada reputasi dan

integritas. Kegagalan dalam mengindahkan ketentuan UU PDP tidak hanya berpotensi menimbulkan konsekuensi hukum yang signifikan, termasuk sanksi administratif dan tuntutan perdata, tetapi juga dapat mengakibatkan kerugian reputasi yang mendalam, erosi kepercayaan pelanggan yang sulit dipulihkan, dan bahkan mengancam stabilitas sistem keuangan secara keseluruhan jika terjadi insiden kebocoran data yang meluas.

Oleh karena itu, investasi dalam teknologi, sumber daya manusia, dan perubahan budaya organisasi yang mendukung pelindungan data pribadi bukan lagi sekadar pilihan, melainkan sebuah keharusan strategis bagi keberlangsungan dan pertumbuhan yang berkelanjutan dalam era digital ini.

Mengatasi Jalinan Kompleksitas dan Merajut Kolaborasi untuk Implementasi UU PDP yang Efektif di Sektor Jasa Keuangan

Tantangan dan hambatan yang dihadapi perusahaan jasa keuangan dalam mengimplementasikan UU PDP dalam sistem informasi mereka terbukti bersifat multidimensional dan saling terkait, merentang dari kompleksitas teknis sistem warisan hingga tantangan interpretasi hukum dan resistensi budaya organisasi. Mengatasi jalinan kompleksitas ini memerlukan pendekatan yang holistik dan kolaboratif, melibatkan tidak hanya upaya internal perusahaan tetapi juga sinergi dengan regulator, penyedia solusi teknologi, dan pemangku kepentingan lainnya.

Modernisasi infrastruktur TI yang mempertimbangkan prinsip *privacy by design* dan *privacy by default*, peningkatan kesadaran dan pemahaman UU PDP di seluruh tingkatan organisasi melalui program pelatihan yang berkelanjutan, alokasi investasi yang memadai untuk teknologi pelindungan data, serta pengembangan kerangka tata kelola data yang kuat merupakan langkah-langkah krusial yang perlu diambil oleh perusahaan jasa keuangan.

Di sisi lain, peran regulator (Otoritas Pelindungan Data Pribadi) menjadi sangat penting dalam menciptakan ekosistem pelindungan data yang kondusif dan efektif di sektor jasa keuangan. Penerbitan peraturan pelaksana dan panduan implementasi yang lebih rinci dan spesifik untuk karakteristik unik industri ini, penegakan hukum yang konsisten dan transparan, serta fasilitasi dialog dan kolaborasi antara regulator dan pelaku industri akan sangat membantu dalam mengatasi ambiguitas interpretasi dan mendorong adopsi praktik terbaik.

Pada akhirnya, implementasi UU PDP yang berhasil dalam sistem informasi perusahaan jasa keuangan akan membutuhkan komitmen jangka panjang, investasi berkelanjutan, dan

kolaborasi yang erat dari seluruh pemangku kepentingan untuk mewujudkan ekosistem keuangan digital yang aman, terpercaya, dan menghormati hak-hak privasi individu.

Saran

Bagi Perusahaan Jasa Keuangan: Perusahaan jasa keuangan di Indonesia perlu mengambil langkah-langkah strategis dan komprehensif untuk memastikan implementasi UU PDP dalam sistem informasi mereka secara efektif. Langkah awal yang krusial adalah melakukan audit mendalam terhadap seluruh sistem informasi dan proses bisnis yang melibatkan pemrosesan data pribadi untuk mengidentifikasi potensi risiko dan kesenjangan kepatuhan terhadap UU PDP. Berdasarkan hasil audit ini, perusahaan perlu menyusun rencana implementasi yang terukur dan bertahap, yang mencakup pengembangan atau pembaruan kebijakan dan prosedur pelindungan data, investasi dalam teknologi keamanan yang relevan (seperti enkripsi, otentikasi multifaktor, dan sistem deteksi intrusi), serta penyelenggaraan program pelatihan dan peningkatan kesadaran yang berkelanjutan bagi seluruh karyawan. Selain itu, penunjukan Data Protection Officer (DPO) yang kompeten dan independen menjadi penting bagi perusahaan yang memenuhi kriteria, untuk mengawasi kepatuhan dan menjadi titik kontak bagi subjek data dan Otoritas Pelindungan Data Pribadi. Perusahaan juga disarankan untuk secara proaktif memantau perkembangan regulasi dan yurisprudensi terkait UU PDP serta beradaptasi dengan perubahan yang mungkin terjadi.

Bagi Regulator (Otoritas Pelindungan Data Pribadi): Otoritas Pelindungan Data Pribadi (ODP) memiliki peran sentral dalam menciptakan ekosistem pelindungan data pribadi yang kondusif di sektor jasa keuangan. Untuk mendukung implementasi UU PDP yang efektif, ODP perlu segera menerbitkan peraturan pelaksana yang lebih rinci dan memberikan panduan yang jelas dan komprehensif mengenai interpretasi pasal-pasal UU PDP, khususnya yang relevan dengan karakteristik unik industri jasa keuangan. Panduan ini sebaiknya mencakup contoh-contoh praktik terbaik, klarifikasi mengenai konsep-konsep kunci seperti "kepentingan yang sah" dan "persetujuan," serta arahan teknis mengenai standar keamanan data yang diharapkan. Selain itu, ODP perlu mengembangkan mekanisme pengawasan dan penegakan hukum yang efektif untuk memastikan kepatuhan terhadap UU PDP dan memberikan efek jera terhadap pelanggaran. Kolaborasi dengan asosiasi industri jasa keuangan dan pemangku kepentingan lainnya juga penting untuk membangun pemahaman bersama dan memfasilitasi pertukaran informasi mengenai tantangan dan solusi implementasi. ODP juga dapat mempertimbangkan untuk mengembangkan program sertifikasi atau standar pelindungan data khusus untuk sektor jasa keuangan guna meningkatkan akuntabilitas dan kepercayaan.

DAFTAR REFERENSI

Accenture. (2023). State of cybersecurity report 2023.

General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

IBM Security. (2023). Cost of a data breach report 2023.

International Organization for Standardization. (n.d.). ISO/IEC 27001: Information security management systems — Requirements.

Makarim, E. (2019). Cyber law: Aspek hukum teknologi informasi. Depok: Rajawali Pers.

PricewaterhouseCoopers. (2023). The future of privacy in financial services [Laporan industri].

Ramli, A. M. (2024). Tantangan implementasi UU PDP di sektor keuangan. Jurnal Hukum Ekonomi dan Bisnis, 5(1), 50–65.

Salim, H. S. (2020). Hukum perlindungan data pribadi di Indonesia. Jakarta: Sinar Grafika.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

World Economic Forum. (2024). The global risks report 2024.