

**IMPLEMENTASI UNDANG-UNDANG PELINDUNGAN DATA PRIBADI:
PERAN MANAJEMEN RISIKO HUKUM BAGI PROSESOR DATA
PRIBADI**
***IMPLEMENTATION OF THE PERSONAL DATA PROTECTION LAW:
THE ROLE OF LEGAL RISK MANAGEMENT FOR PERSONAL DATA
PROCESSORS***

Tiara Shafa Putri dan Moody Rizqy Syailendra Putra

Fakultas Hukum Universitas Tarumanagara

Korespondensi Penulis : tiara.205210002@stu.untar.ac.id

Citation Structure Recommendation :

Putri, Tiara Shafa dan Moody Rizqy Syailendra Putra. *Implementasi Undang-Undang
Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi*. Jurnal
Hukum Lex Generalis. Vol.5. No.4 (2024)

ABSTRAK

Dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pengaturan mengenai pelindungan data pribadi semakin bertambah dan berkembang. Implementasi UU PDP memberikan kepastian hukum mengenai kegagalan pelindungan data pribadi di Indonesia. Metode penilitan yang digunakan dalam penulisan ini adalah metode hukum normatif dengan menganalisis bahan hukum yaitu UU PDP untuk menyelesaikan isu yang dibahas. Serta mengacu pada bahan lain seperti buku, jurnal, ataupun artikel yang berkaitan dengan pelindungan data pribadi. Tujuan penelitian ini adalah untuk memahami tantangan saat pengimplementasian UU 27/2022 dan peran manajemen risiko selama proses implementasi. Tantangan dalam pengimplementasian UU 27/2022 adalah masih banyak elemen-elemen yang disebutkan dalam UU 27/2022 yang belum eksis sampai sekarang. Seperti peraturan-peraturan turunan yang nantinya menjadi peraturan pelaksanaan dan juga lembaga pelindungan data pribadi. Lalu manajemen risiko hukum memiliki peran yang penting dalam membantu prosesor data pribadi untuk mengidentifikasi, mengelola, dan memitigasi risiko hukum terkait kebocoran data, ketidakpatuhan terhadap regulasi, serta potensi tuntutan hukum dari subjek data.

Kata Kunci: Hukum Perlindungan Data Pribadi, Manajemen Risiko Hukum, Pelindungan Data Pribadi, Prosesor Data Pribadi

ABSTRACT

With the enactment of Law Number 27 of 2022 concerning Personal Data Protection (Law No. 27/2022), the regulations governing personal data protection have expanded and developed significantly. The implementation of the Law No. 27/2022 provides legal certainty regarding failures in personal data protection in Indonesia. This research employs a normative legal methodology, analyzing legal materials such as the Law No. 27/2022 to address the issues discussed. It also references other materials, including books, journals, and articles related to personal data protection. The purpose of this study is to understand the challenges in implementing the Law No. 27/2022 and the role of risk management during the implementation process. One of the challenges in implementing the Law No. 27/2022 is the absence of several elements mentioned in the law to date, such as implementing regulations that serve as derivative rules and the establishment of a personal data protection authority. Legal risk management plays a crucial role in assisting personal data processors in identifying, managing, and mitigating legal risks associated with data breaches, regulatory non-compliance, and potential legal claims from data subjects.

Keywords: *Personal Data Protection Law, Legal Risk Management, Private Data, Private Data Processor*

A. PENDAHULUAN

1. Latar Belakang

Pada era digital ini, informasi berkembang dan tersebar luas dengan sangat cepat. Hal tersebut memberikan dampak kepada cara bertransaksi dan berkomunikasi di dunia media sosial. Perkembangan di era ini berkaitan erat dengan topik yang sudah muncul dari lama yaitu perlindungan data pribadi. Data pribadi erat kaitannya dengan hak privasi. Dimana hak privasi telah diakui sebagai salah satu bagian dari hak asasi manusia oleh Mahkamah Konstitusi melalui putusan No.5/PUU-VIII/2011.¹ Hak privasi merupakan salah satu hak mutlak yang dimiliki manusia untuk dilindungi. Hak privasi diartikan sebagai “*the right to personal autonomy*”.² Samuel Warren dan Louis Brandeis mengartikan pribadi sebagai “*right to be let alone*” atau yang artinya hak untuk dibiarkan sendiri.³

Data pribadi yang termasuk ke dalam hak privasi telah menjadi bahasan di dunia internasional sejak lama. Salah satu peraturan mengenai perlindungan data pribadi adalah *European Union General Data Protection Regulation* (yang untuk selanjutnya disebut dengan “**GDPR**”) yang mengartikan Data pribadi (*personal data*) sebagai semua informasi yang dapat mengidentifikasi seseorang (*data subject*). Yang termasuk ke dalam data pribadi adalah nama, nomor induk kependudukan, data lokasi, dan informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.⁴ Di Indonesia sendiri, telah terjadi banyak kegagalan perlindungan data pribadi yang melibatkan institusi-institusi pemerintahan seperti Pusat Data Nasional Sementara yang terkena serangan siber dan menyebabkan data kementerian dan lembaga, serta pemerintah provinsi, kabupaten, dan kota mengalami kebocoran dan memberikan dampak pada 282 instansi pemerintah.⁵

¹ Yovita Arie Mangesti, dkk., *Ethico-Legal Aspects Of Personal Data Protection In Indonesia*, International Journal of Educational Research & Social Sciences, Vol.2, No.5 (2021), p.1032.

² Bryan A. Garner (eds), *Black's Law Dictionary 7th Edition*, West Publishing Co, St. Paul Minnesota, 2004, p.74-75.

³ Samuel D. Warren dan Louis Brandeis, *The Right to Privacy*, Harvard Law Review, Vol.4 (1890), p.193.

⁴ European Union, *The General Data Protection Regulation*, Ps.4 ayat (1).

⁵ Viriya Singgih, *Pentingnya Kominformo Mundur 'Sebagai Tanggung Jawab Moral' Setelah Pusat Data Nasional Diretas*, diakses dari <https://www.bbc.com/indonesia/articles/c8vdmymynzo#:~:text=Per%2026%20Juni%2C%20pe merintah%20mencatat,segera%20pulihan%20karena%20memiliki%20backup>, diakses pada 30 Desember 2024.

Tiara Shafa Putri dan Moody Rizqy Syailendra Putra
Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi

Selain itu, BPJS Kesehatan juga pernah mengalami kebocoran data pribadi yang menyebabkan dijualnya 279 juta data penduduk Indonesia diperjualbelikan melalui forum internet bernama *Raid Forum*.⁶

Indonesia selaku negara melakukan kewajibannya dalam melindungi warga negaranya melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (yang untuk selanjutnya disebut dengan “UU 27/2022”). Melalui pengesahan ini, pelindungan data pribadi di Indonesia menjadi semakin berkembang sebab sebelum UU 27/2022 ini disahkan, belum ada peraturan perundang-undangan setara undang-undang yang mengatur khusus tentang pelindungan data pribadi.⁷ Data pribadi menurut UU 27/2022 adalah data yang dapat mengidentifikasi seseorang. Contohnya adalah nomor telepon, alamat tempat tinggal, agama, Nomor Induk Kependudukan (NIK), dan lain-lain. Sehingga kegagalan pelindungan data pribadi dapat memberikan kerugian bagi subjek data pribadi seperti penyalahgunaan data untuk hal yang dilarang, pencurian identitas, atau bahkan penipuan yang melibatkan finansial.⁸ Oleh karena itu, data pribadi perlu dilindungi agar terhindar dari tindakan penyalahgunaan dan tindakan lainnya yang dapat merugikan subjek data pribadi.⁹

UU 27/2022 menetapkan berbagai ketentuan yang harus dipatuhi oleh pengendali data maupun prosesor data pribadi, termasuk mekanisme persetujuan subjek data, kewajiban melaporkan pelanggaran data, serta pengelolaan hak-hak subjek data seperti hak akses, hak perbaikan, dan hak penghapusan data. Regulasi ini dirancang untuk memperkuat sistem pelindungan data pribadi namun pengimplementasinya tidaklah mudah. Terutama bagi prosesor data pribadi yang merupakan pihak yang ditunjuk oleh pengendali data untuk memproses data sesuai dengan instruksi tertentu. Melalui beberapa pasal dalam UU 27/2022, prosesor data pribadi memiliki kewajiban dalam penerapan UU 27/2022.

⁶ Abd Rahman Saleh, *Perlindungan Data Pribadi dalam Prespektif Kebijakan Hukum Pidana*, Hukmy: Jurnal Hukum, Vol.1, No.1 (2021), p.1.

⁷ Moody Rizqy Syailendra, dkk., *Personal Data Protection Law In Indonesia: Challenges and Opportunities*, Indonesia Law Review, Vol.14, No.2 (2024), p.58.

⁸ Rachel Milafebina, dkk., *Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-Commerce di Indonesia*, Jurnal Tana Mana, Vol.4, No.1 (April 2021), p.158.

⁹ Moody Rizqy Syailendra, *Perlindungan Data Pribadi terhadap Tindakan Penyebaran Sex Tape Menurut Hukum Positif di Indonesia*, Jurnal Muara Ilmu Sosial, Humaniora, dan Seni, Vol.5, No.2 (2021), p.441.

Tidak menutup kemungkinan dalam melaksanakan kewajiban tersebut, terdapat berbagai tantangan yang perlu dihadapi. Salah satunya adalah mengenai pemahaman yang belum matang mengenai kewajibannya. Tidak semua organisasi atau badan yang berperan sebagai prosesor data pribadi memiliki sumber daya yang memadai untuk mematuhi aturan. Selain itu, tantangan lain yang kemungkinan perlu dihadapi adalah keterbatasan teknologi, keterbatasan tenaga ahli, dan lain-lain.

Dalam menghadapi tantangan tersebut, manajemen risiko berperan dalam membantu organisasi atau badan untuk mengidentifikasi, mengelola, dan memitigasi risiko yang mungkin timbul dari kegiatan pemrosesan data. Manajemen risiko hukum tidak hanya berfokus pada penyusunan kebijakan internal yang sesuai dengan undang-undang, tetapi juga mencakup pelatihan dan edukasi karyawan, audit reguler, serta pengawasan terhadap perubahan regulasi. Implementasi UU 27/2022 di Indonesia memerlukan manajemen risiko hukum yang efektif untuk memastikan kepatuhan prosesor data terhadap aturan perlindungan data pribadi. Prosesor data pribadi harus mengelola potensi risiko hukum melalui kebijakan internal, teknologi keamanan seperti enkripsi, dan pelatihan karyawan. Hal ini penting untuk menghindari sanksi administratif, pidana, atau kerugian reputasi akibat pelanggaran data. Adapun rumusan masalah dalam penelitian ini:

- a. Bagaimana tantangan dalam pengimplementasian Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi bagi prosesor data pribadi?
- b. Bagaimana peran manajemen risiko hukum dalam proses pengimplementasian Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi bagi prosesor data pribadi?

Penelitian ini menggunakan metode hukum normatif yaitu menganalisis regulasi yang sesuai dengan isu yang dibahas. Regulasi yang digunakan dalam penelitian ini yang utama adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dilanjutkan dengan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik sebagai acuan ataupun pembandingan aturan perlindungan data pribadi. Selain menggunakan undang-undang, penelitian ini juga menggunakan bahan lain seperti buku, jurnal, artikel, berita, dan lain-lain sebagai acuan penulisan.

B. PEMBAHASAN

1. Tantangan dalam Pengimplementasian UU 27/2022

Pengesahan UU 27/2022 memberikan sedikit titik terang menyangkut masalah kegagalan pelindungan data pribadi di Indonesia sebab sebelum UU 27/2022 disahkan, tidak jarang terjadi peristiwa kegagalan pelindungan data pribadi yang mengancam hak privasi warga negara.¹⁰ Disahkannya UU 27/2022 ini mendukung peran Indonesia sebagai negara dalam melindungi kepentingan warga negaranya seperti yang diatur dalam Pasal 28G Undang-Undang Dasar Republik Indonesia Tahun 1945. Dimana pasal tersebut menyatakan bahwa setiap hak warga negara perlu dilindungi oleh negaranya. Namun, dalam pengimplementasian UU 27/2022 ini masih banyak hal-hal yang menjadi tantangan bagi para pihak terkait. Diatur dalam Pasal 1 angka 5 bahwa salah satu pihak yang berkaitan erat dengan pelindungan data pribadi adalah prosesor data pribadi. Prosesor data pribadi diartikan sebagai pihak yang melakukan pemrosesan data pribadi atas nama pengendali data pribadi. Prosesor data pribadi dapat berupa orang, badan publik, maupun organisasi internasional. Melalui UU 27/2022, kewajiban prosesor data pribadi diatur dalam rangka mewujudkan pelindungan data pribadi yang sesuai dengan regulasi.

Kewajiban prosesor data pribadi diatur dalam Pasal 51 sampai dengan Pasal 53 UU 27/2022.¹¹ Dimana kewajiban prosesor data pribadi tidak jauh berbeda dengan kewajiban pengendali data pribadi. Dimana pada dasarnya yang menjadi kewajiban prosesor data pribadi adalah sebagai berikut:¹²

- a. Prosesor data pribadi diwajibkan untuk memastikan akurasi, kelengkapan, dan konsistensi data pribadi dengan melakukan verifikasi (Pasal 29)

¹⁰ Juan Matheus dan Ariawan Gunadi, *Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU*, JUSTISI, Vol.10, No.1 (2023), p.23.

¹¹ Indonesia, *Undang-Undang tentang Pelindung Data Pribadi*, UU No.27 Tahun 2022, LN Tahun 2022 No.196, TLN No.6820, Ps.51-53.

¹² Jonathan Matthew, *Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*, Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat, Vol.10, No.1 (2024), p.119-137

- b. Melakukan perekaman saat pemrosesan data pribadi (Pasal 31)
- c. Melindungi dan memastikan keamanan data pribadi yang diproses dengan melakukan (Pasal 35):
 - 1) Penyusunan dan penerapan langkah teknis operasional
 - 2) Penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko
- d. Menjaga kerahasiaan data pribadi (Pasal 36).
- e. Pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan (Pasal 37)
- f. Melindungi dari pemrosesan yang tidak sah (Pasal 38).
- g. Mencegah akses data pribadi yang tidak sah dengan menggunakan sistem keamanan dan sistem elektronik yang andal, aman, dan bertanggungjawab (Pasal 39)

Prosesor data pribadi dalam melaksanakan kewajibannya sesuai dengan UU 27/2022 perlu menghadapi beberapa tantangan. Salah satu yang menjadi tantangan terbesar adalah kurangnya pemahaman dan kepatuhan terhadap UU 27/2022. UU 27/2022 memuat berbagai ketentuan teknis yang memerlukan penerjemahan ke dalam kebijakan operasional, seperti pengelolaan hak subjek data, mekanisme pelaporan pelanggaran, dan persetujuan untuk pemrosesan data sensitif. Pada realitanya, banyak organisasi belum memahami cara menangani permintaan hak akses, perbaikan, atau penghapusan data oleh subjek data, sehingga sering terjadi ketidaksesuaian dengan regulasi sebab dalam pengimplementasian UU 27/2022, organisasi atau badan masih perlu menghadapi tantangan dari berbagai aspek yaitu regulasi, infrastruktur, hingga sumber daya manusia, berbagai tantangan ini membutuhkan perhatian serius untuk memastikan kepatuhan terhadap UU 27/2022. Tantangan yang dihadapi dapat berupa ketidaksiapan teknologi, kurangnya pemahaman atas perlindungan data pribadi, dan koordinasi yang lemah antara pengendali data pribadi dengan prosesor data pribadi.¹³

¹³ Wanda Dwi Cahyani dan Anita Marianata, *Analisis Kebijakan Perlindungan Data Pribadi di Kota Bengkulu: Studi Implementasi UU PDP dalam Era Digital*, Jurnal Kajian Hukum dan Kebijakan Publik, Vol.2, No.1 (2024), p.623-626.

Kondisi ini terutama dialami oleh organisasi kecil atau menengah yang belum memiliki sistem tata kelola data yang mapan. Selain kurangnya pemahaman, yang menjadi tantangan lain adalah keterbatasan teknologi. Khususnya bagi mereka organisasi atau badan kecil seperti contoh UMKM. Banyak UMKM yang merasa kesulitan untuk mengadakan anggaran untuk keperluan teknologi karena membutuhkan biaya yang tidak sedikit. Tanpa teknologi yang memadai, data pribadi yang mereka kelola menjadi lebih rentan terhadap kebocoran dan ancaman serangan siber, yang tidak hanya merugikan individu pemilik data tetapi juga dapat menyebabkan sanksi berat bagi prosesor data pribadi atau UMKM tersebut. Keterbatasan sumber daya manusia juga menjadi tantangan yang sangat signifikan. Pada saat ini, jumlah tenaga kerja yang paham mengenai aturan pelindungan data pribadi di Indonesia masih terbatas sehingga berpengaruh terhadap proses pengimplementasian UU 27/2022. Selain itu, kurangnya pelatihan teknis untuk staf operasional sering kali membuat mereka kesulitan mengikuti standar pengelolaan data yang ditetapkan oleh UU 27/2022. Oleh karena itu, perlu adanya tindakan atas urgensi Tantangan lainnya adalah kurang kerjasama atau koordinasi antara pengendali data pribadi dan prosesor data pribadi, dimana pengendali data pribadi bertanggungjawab atas keselarasan antara pemrosesan data pribadi di lapangan dengan UU 27/2022. Perbedaan interpretasi kebijakan dan kurangnya komunikasi yang efektif antara kedua pihak sering kali menyebabkan konflik dan ketidakpatuhan.

Pelanggaran terhadap kewajiban yang diatur dalam UU 27/2022 menghadirkan ancaman serius berupa sanksi administratif maupun pidana.¹⁴ Ketentuan ini memberikan tekanan yang signifikan, khususnya bagi organisasi berskala kecil dan menengah. UU 27/2022 menetapkan bahwa pelanggaran terhadap kewajiban perlindungan data pribadi dapat berujung pada pengenaan denda administratif yang nilainya mencapai 2% dari pendapatan tahunan organisasi yang bersangkutan.

¹⁴ Hari Sutra Disemadi, dkk., *Pelindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?*, Sang Sewagati Journal, Vol.1, No.2 (2023), p.66-90.

Besarnya ancaman sanksi tersebut kerap menimbulkan kekhawatiran di kalangan pengelola data pribadi, terutama para prosesor data. Rasa khawatir ini dapat memengaruhi pengambilan keputusan mereka, bahkan mengakibatkan penundaan dalam melakukan investasi strategis yang sebenarnya diperlukan untuk memastikan kepatuhan terhadap aturan perlindungan data. Situasi ini menunjukkan adanya tantangan nyata dalam menciptakan keseimbangan antara pemberlakuan aturan hukum yang tegas dan upaya mendukung keberlanjutan organisasi, khususnya yang memiliki keterbatasan sumber daya.

Guna menghadapi tantangan-tantangan ini, perlu adanya peningkatan pemahaman bagi para organisasi yang menjadi prosesor data pribadi. Selain itu, terjalin kerja sama yang baik antara organisasi dengan pemerintah juga merupakan langkah yang penting. Dimana pemerintah dapat menunjukan dukungan kepada organisasi selaku prosesor data pribadi untuk patuh pada aturan dengan memberikan insentif melalui subsidi pengadaan teknologi, penyediaan panduan teknis yang jelas dan pelatihan terstruktur yang dapat membantu organisasi memahami kewajibannya dalam UU 27/2022.

2. Peran Manajemen Risiko Hukum

Di tengah pesatnya digitalisasi, elemen strategis dalam menjamin kepatuhan terhadap UU 27/2022 adalah manajemen risiko hukum. Metode ini membantu perusahaan mengelola data secara aman dan transparan karena mencakup identifikasi potensi risiko, pembuatan kebijakan internal, dan pengelolaan dampak keuangan dan reputasi. Proses ini tidak hanya melindungi, tetapi juga proaktif untuk meningkatkan kepercayaan publik dan menjaga akuntabilitas pengelolaan dan pemrosesan data pribadi.

a. Identifikasi Risiko Hukum

Peran utama dari manajemen risiko hukum adalah mengidentifikasi kemungkinan risiko yang dapat menyebabkan pelanggaran terhadap UU 27/2022. Manajemen risiko berkaitan erat dengan proses analisis mendalam terhadap seluruh kegiatan pemrosesan data, termasuk pengumpulan, penyimpanan, & distribusi data pribadi. Kelemahan dalam manajemen data, seperti kurangnya enkripsi atau mekanisme autentikasi,

dapat meningkatkan risiko kebocoran data. Selain itu, pengabaian terhadap hak subjek data sering menjadi sumber risiko hukum dalam kasus kebocoran data pribadi. Organisasi yang gagal mengidentifikasi kemungkinan risiko memiliki kemungkinan yang lebih besar untuk terkena sanksi administratif maupun pidana sehingga manajemen risiko hukum memiliki peran yang penting dalam menghindari terjadinya kegagalan pelindungan data pribadi yang akan dikenakan sanksi.

b. Perancangan Kebijakan Internal

Manajemen risiko hukum juga bertanggung jawab dalam merancang kebijakan internal yang sesuai dengan regulasi UU 27/2022. Kebijakan ini mencakup prosedur untuk memperoleh persetujuan eksplisit dari subjek data, mekanisme pelaporan pelanggaran, dan tata cara pemenuhan permintaan subjek data terkait pengelolaan data pribadinya. Adanya kebijakan internal yang baik dapat membantu organisasi dalam meminimalisir terjadinya risiko kegagalan pelindungan data pribadi. Selain itu, kebijakan ini harus dikomunikasikan secara jelas kepada seluruh pihak yang terlibat agar dapat diimplementasikan secara konsisten.

c. Pelatihan

Pelatihan dan edukasi karyawan menjadi bagian integral dari manajemen risiko hukum. Melalui pelatihan, tenaga kerja akan mendapat kesadaran dan pemahaman mengenai kewajiban mereka selaku prosesor data pribadi pada UU 27/2022 sehingga mereka dapat melakukan pelindungan data pribadi organisasi sesuai dengan yang diatur. Namun pelatihan ini perlu juga mencakup tentang konsekuensi hukum atau sanksi baik sanksi administrasi maupun pidana jika sekiranya terjadi kegagalan pelindungan data pribadi, serta perlunya langkah-langkah preventif agar organisasi terhindar dari kegagalan pelindungan data pribadi. Pelatihan dan edukasi perlu dilakukan secara berkala dan berkelanjutan agar tenaga kerja dan organisasinya tetap dapat mengikuti perkembangan regulasi yang menyangkut dengan kegiatan pemrosesan data pribadi.

d. Implementasi Prosedur Kepatuhan

Manajemen risiko hukum memastikan adanya prosedur operasional yang jelas untuk menjaga kepatuhan terhadap UU 27/2022. Prosedur operasional ini termasuk audit, pencatatan kegiatan pemrosesan data pribadi, dan langkah-langkah preventif dalam menangani kegagalan perlindungan data pribadi. Prosedur operasional yang jelas dapat mendukung organisasi untuk patuh kepada UU 27/2022 maupun lembaganya sekaligus meminimalisir risiko terkena sanksi. Pencatatan kegiatan pemrosesan yang baik juga menjadi alat penting untuk menunjukkan kepatuhan dalam proses audit.

e. Pengelolaan Risiko Keuangan dan Reputasi

Organisasi yang melakukan pelanggaran terhadap perlindungan data pribadi mengakibatkan turunnya rasa kepercayaan publik yang dapat berdampak pada jangka panjang sehingga peran manajemen risiko hukum disini adalah membantu meminimalisir terjadinya kemungkinan risiko agar organisasi terhindar dari kegagalan data pribadi yang dapat menyebabkan hilangnya kepercayaan publik dan berdampak pada keuangan organisasi dan reputasi organisasi yang tercoreng.

f. Pengawasan dan Penyesuaian Aturan

Aturan terkait perlindungan data pribadi terus berkembang, baik di tingkat nasional maupun internasional. Oleh karena itu, manajemen risiko hukum harus memantau perubahan aturan dan menyesuaikan kebijakan internal secara cepat untuk tetap sesuai dengan aturan terbaru. Pengawasan dan penyesuaian ini perlu adanya kerja sama yang baik antar divisi untuk memastikan implementasi aturan yang terbaru. Khususnya jika organisasi tersebut melakukan kegiatan operasional lintas batas, di mana aturan internasional juga mempengaruhi kegiatan pemrosesan data pribadi mereka.

Dengan metode manajemen risiko hukum, organisasi tidak hanya meningkatkan kepatuhan terhadap hukum, tetapi juga membangun kerangka kerja yang kokoh untuk melindungi hak-hak subjek data secara berkelanjutan.

Tiara Shafa Putri dan Moody Rizqy Syailendra Putra
Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi

Identifikasi risiko hukum yang mendalam memungkinkan organisasi memahami kemungkinan risiko dalam kegiatan pemrosesan data pribadi. Dengan langkah ini, organisasi dapat mengembangkan strategi mitigasi yang tepat, seperti penguatan enkripsi, peningkatan kontrol akses, dan pengawasan ketat terhadap proses pengumpulan data pribadi.

Oleh karena itu, penyusunan kebijakan internal yang sesuai dengan regulasi membantu menciptakan tata kelola data yang terorganisir dan terstruktur. Kebijakan ini mencakup pedoman teknis yang tidak hanya berorientasi pada pemenuhan peraturan, tetapi juga memperhatikan aspek etika dalam pengelolaan dan pemrosesan data pribadi. Dengan mendokumentasikan kegiatan tersebut secara sistematis, organisasi dapat memberikan jaminan kepatuhan kepada otoritas berwenang, mitra bisnis, dan publik. Pelatihan karyawan menjadi elemen kunci dalam implementasi manajemen risiko hukum. Program edukasi yang berkelanjutan meningkatkan kesadaran terhadap pentingnya pelindungan data pribadi, sekaligus memperkuat kepatuhan dalam organisasi. Selain itu, langkah ini juga memastikan bahwa seluruh tim memahami konsekuensi hukum dan reputasi dari pelanggaran, sehingga mereka mampu mengambil tindakan pencegahan.

Manajemen risiko hukum yang efektif juga mendorong pengembangan prosedur operasional yang transparan, seperti audit dan mekanisme respon tanggap darurat. Prosedur ini tidak hanya membantu organisasi dalam meminimalkan risiko denda atau sanksi administratif, tetapi juga menciptakan kepercayaan publik terhadap pengelolaan dan pemrosesan data pribadi. Kepercayaan ini menjadi aset berharga dalam membangun hubungan jangka panjang dengan konsumen, mitra bisnis, dan stakeholder lainnya. Selain itu, risiko keuangan dan reputasi yang terkait dengan pelanggaran data dapat diminimalkan melalui strategi pengelolaan risiko yang terencana. Misalnya, organisasi dapat memanfaatkan asuransi pelindungan data pribadi untuk mengurangi dampak finansial, sekaligus mengembangkan strategi komunikasi krisis untuk menjaga reputasi. Pendekatan ini memastikan bahwa organisasi tetap beroperasi secara optimal meskipun menghadapi situasi sulit.

Dengan pengawasan regulasi yang konsisten dan kemampuan untuk beradaptasi terhadap perubahan peraturan, organisasi dapat mempertahankan relevansi dan kepatuhan mereka terhadap standar perlindungan data pribadi yang terus berkembang. Melalui pendekatan ini, organisasi tidak hanya memenuhi kewajiban hukum, tetapi juga memberikan kontribusi pada penguatan ekosistem perlindungan data yang lebih andal, baik di tingkat nasional maupun internasional. Manajemen risiko hukum yang dijalankan secara proaktif, komprehensif, dan terstruktur memberikan manfaat jangka panjang bagi organisasi. Selain mengurangi kemungkinan sanksi, pendekatan ini juga memperkuat daya saing organisasi dalam ekonomi digital yang semakin mengutamakan transparansi, akuntabilitas, dan kepercayaan publik.

C. PENUTUP

1. Kesimpulan

Berdasarkan analisis yang dilakukan dalam penelitian ini, dapat disimpulkan bahwa implementasi UU 27/2022 merupakan langkah penting dalam upaya melindungi hak privasi individu dan membangun ekosistem digital yang lebih aman dan terpercaya di Indonesia. Namun, meskipun UU 27/2022 diharapkan dapat memberikan perlindungan yang lebih baik, implementasinya menghadirkan berbagai tantangan, terutama bagi prosesor data pribadi yang menjadi pihak yang bertanggung jawab dalam pengelolaan data pribadi. Tantangan utama yang dihadapi prosesor data pribadi adalah kurangnya pemahaman yang memadai tentang kewajiban yang diatur dalam UU 27/2022, keterbatasan infrastruktur teknologi, serta kurangnya sumber daya manusia yang memiliki kompetensi dalam manajemen data pribadi. Selain itu, masih terdapat kendala dalam koordinasi yang kurang efektif antara pengendali dan prosesor data, yang mengakibatkan ketidakpatuhan terhadap regulasi dan potensi konflik dalam interpretasi kebijakan. Ancaman sanksi administratif dan pidana yang diatur juga menciptakan tekanan besar bagi prosesor data, khususnya bagi perusahaan kecil dan menengah yang belum memiliki kapasitas untuk memenuhi persyaratan yang telah ditetapkan.

Oleh karena itu, untuk mengatasi tantangan ini, diperlukan pendekatan strategis yang melibatkan kerja sama antara pemerintah, pengendali data, prosesor data, serta masyarakat untuk meningkatkan kesadaran, membangun infrastruktur yang memadai, dan menyediakan pelatihan yang efektif.

Manajemen risiko hukum memegang peran kunci dalam menghadapi tantangan ini. Dengan pendekatan sistematis yang melibatkan identifikasi dan mitigasi risiko hukum, penyusunan kebijakan internal yang sesuai dengan ketentuan UU 27/2022, serta pelatihan dan edukasi bagi staf operasional. Manajemen risiko hukum dapat membantu prosesor data pribadi untuk meminimalisir risiko pelanggaran, meningkatkan kepatuhan, dan melindungi reputasi organisasi. Selain itu, pengawasan yang berkelanjutan dan penerapan teknologi yang mendukung pengelolaan data pribadi yang aman juga menjadi aspek penting dalam memastikan keberhasilan implementasi UU 27/2022.

2. Saran

Berdasarkan temuan dalam penelitian ini, beberapa saran dapat diajukan untuk meningkatkan implementasi UU 27/2022 dan memperkuat peran manajemen risiko hukum, antara lain:

a. Peningkatan Literasi Data dan Pelatihan Kepatuhan

Perlu diadakan pelatihan dan sosialisasi terkait isi dari UU 27/2022, agar terdapat peningkatan pemahaman tentang aturan ini. Pelatihan yang efektif tidak hanya akan meningkatkan pengetahuan tentang kewajiban hukum, tetapi juga membantu prosesor data pribadi dalam merancang dan mengimplementasikan kebijakan yang sesuai. Pemerintah juga diharapkan dapat menyediakan materi pelatihan dan sumber daya yang dapat diakses oleh semua jenis organisasi.

b. Penguatan Infrastruktur Teknologi

Prosesor data pribadi, terutama dari sektor UMKM, perlu dukungan pembangunan infrastruktur teknologi memadai untuk memastikan perlindungan data pribadi yang maksimal. Pemerintah dapat memberikan insentif/subsidi guna mendorong perusahaan untuk berinvestasi dalam teknologi keamanan data, seperti enkripsi dan sistem deteksi intrusi, agar data pribadi dapat terlindungi dari potensi kebocoran dan serangan siber.

c. Kerja Sama yang Lebih Baik antara Pengendali dan Prosesor Data Pribadi

Guna meningkatkan kepatuhan terhadap UU 27/2022, perlu adanya upaya yang lebih besar dalam memperbaiki koordinasi dan komunikasi antara pengendali dan prosesor data. Pengendali data harus memastikan bahwa prosesor data pribadi memiliki pemahaman yang jelas tentang kewajiban yang harus dipenuhi dan memberikan panduan yang komprehensif dalam pengelolaan data pribadi. Prosesor data pribadi, di sisi lain, harus dapat memastikan bahwa mereka mematuhi kebijakan dan prosedur yang ditetapkan oleh pengendali data pribadi.

d. Implementasi Sistem Manajemen Risiko yang Terstruktur

Organisasi harus mengembangkan sistem manajemen risiko hukum yang terstruktur dan sistematis untuk mengidentifikasi dan mengelola potensi risiko yang berkaitan dengan perlindungan data pribadi. Dengan adanya kebijakan internal yang jelas, prosedur operasional standar yang dapat diikuti, serta pelatihan yang rutin, prosesor data pribadi akan lebih siap dalam menghadapi tantangan dan risiko yang timbul. Sistem manajemen risiko hukum ini juga dapat membantu organisasi dalam memitigasi kemungkinan risiko pelanggaran yang dapat berujung pada sanksi administratif maupun pidana.

e. Penegakan Hukum yang Konsisten dan Adil

Untuk mendukung keberhasilan implementasi UU 27/2022, penegakan hukum yang konsisten dan adil sangat diperlukan Pemerintah dan lembaga terkait harus memastikan bahwa sanksi terhadap pelanggaran perlindungan data pribadi diterapkan secara tegas dan adil, dengan mempertimbangkan kapasitas dan karakteristik masing-masing organisasi. Selain itu, upaya preventif seperti pengawasan dan audit juga perlu dilakukan untuk memastikan bahwa organisasi mematuhi kewajiban mereka sesuai dengan UU 27/2022.

Dengan menerapkan langkah-langkah tersebut, diharapkan UU 27/2022 dapat diimplementasikan dengan lebih efektif, memberikan perlindungan yang lebih baik bagi data pribadi masyarakat Indonesia, serta memperkuat kepercayaan publik terhadap sistem digital yang ada.

Tiara Shafa Putri dan Moody Rizqy Syailendra Putra
Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi

Implementasi UU 27/2022 yang efektif akan memastikan bahwa data pribadi yang dimiliki oleh individu terlindungi dengan baik, mencakup pengaturan yang jelas mengenai pengumpulan, pemrosesan, penyimpanan, dan penggunaan data pribadi, serta hak individu untuk mengakses, memperbaiki, atau menghapus data mereka. Dengan adanya perlindungan yang lebih baik, masyarakat akan merasa lebih aman dalam berinteraksi dengan platform digital, mengetahui bahwa data mereka tidak disalahgunakan atau tersebar tanpa izin.

Kepercayaan publik sangat penting dalam penggunaan teknologi digital, dan ketika masyarakat melihat bahwa data pribadi mereka dilindungi dengan baik melalui implementasi UU 27/2022 yang tegas, mereka akan lebih percaya untuk berpartisipasi dalam kegiatan digital seperti transaksi *online*, penggunaan media sosial, dan berbagai aplikasi berbasis data lainnya. Kepercayaan ini juga memperkuat ekosistem digital secara keseluruhan, menciptakan hubungan yang lebih transparan antara pengguna dan penyedia layanan. Selain itu, keberhasilan implementasi UU 27/2022 tidak hanya mempengaruhi perlindungan individu, tetapi juga menciptakan standar pengelolaan data yang lebih baik di tingkat nasional. Organisasi dan perusahaan yang mematuhi UU 27/2022 akan berkontribusi pada terciptanya praktik pengelolaan data yang lebih aman dan bertanggung jawab, yang pada gilirannya akan mendorong terciptanya lingkungan digital yang lebih terpercaya. Hal ini juga berpotensi meningkatkan daya saing Indonesia di tingkat global, terutama dalam bidang perlindungan data pribadi, yang semakin penting di dunia yang semakin terhubung secara digital.

DAFTAR PUSTAKA

Buku

Garner, Bryan A. (eds). (2004). *Black's Law Dictionary 7th Edition*. (St. Paul Minnesota: West Publishing Co).

Publikasi Ilmiah

Cahyani, Wanda Dwi dan Anita Marianata. *Analisis Kebijakan Perlindungan Data Pribadi di Kota Bengkulu: Studi Implementasi UU PDP dalam Era Digital*. Jurnal Kajian Hukum dan Kebijakan Publik. Vol.2. No.1 (2024).

Mangesti, Yovita Arie. dkk.. *Ethico-Legal Aspects Of Personal Data Protection In Indonesia*. International Journal of Educational Research & Social Sciences. Vol.2. No.5 (2021).

Matheus, Juan dan Ariawan Gunadi. *Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU*. JUSTISI. Vol.10. No.1 (2023).

Matthew, Jonathan. *Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat. Vol.10. No.1 (2024).

Milafebina, Rachel. dkk.. *Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-Commerce di Indonesia*. Jurnal Tana Mana. Vol.4. No.1 (April 2021).

Saleh, Abd Rahman. *Perlindungan Data Pribadi dalam Prespektif Kebijakan Hukum Pidana*. Hukmy: Jurnal Hukum. Vol.1. No.1 (2021).

Syailendra, Moody Rizqy. dkk.. *Personal Data Protection Law In Indonesia: Challenges and Opportunities*. Indonesia Law Review. Vol.14. No.2 (2024).

Syailendra, Moody Rizqy. *Perlindungan Data Pribadi terhadap Tindakan Penyebaran Sex Tape Menurut Hukum Positif di Indonesia*. Jurnal Muara Ilmu Sosial, Humaniora, dan Seni. Vol.5. No.2 (2021).

Warren, Samuel D. dan Louis Brandeis. *The Right to Privacy*. Harvard Law Review. Vol.4 (1890).

Website

Singgih, Viriya. *Petinggi Kominfo Mundur 'Sebagai Tanggung Jawab Moral' Setelah Pusat Data Nasional Diretas*. diakses dari <https://www.bbc.com/indonesia/articles/c8vdmymynzo#:~:text=Per%2026%20Juni%2C%20pemerintah%20mencatat,segera%20pulihan%20karena%20memiliki%20backup>. diakses pada 30 Desember 2024.

Sumber Hukum

The General Data Protection Regulation.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.