p-ISSN: 2963-7856| e-ISSN: 2961-9890
Available online at jerkin.org/index.php/jerkin
Jurnal Pengabdian Masyarakat dan Riset Pendidikan
Volume 4 No. 3, Januari-Maret 2026, pp 16034-16040

Tanggung Jawab Hukum Korporasi Atas Kebocoran Data Peserta BPJS Kesehatan Berdasarkan UU No. 27 Tahun 2022

Ridho Rivantoro[1]*, Dyah Permata Budi Asri[2]
[1,2] Fakultas Hukum, Universitas Esa Unggul, Jl. Arjuna Utara No.9, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta.
E-mail: rrivantoro1997@gmail.com
* Corresponding Author

https://doi.org/10.31004/jerkin.v4i3.4575

ARTICLE INFO

Article history:
Received: 21 Dec 2025
Revised: 27 Dec 2025
Accepted: 02 Jan 2026

Kata Kunci:
BPJS Kesehatan, Data Pribadi, Pelanggaran Data, Korporasi, Hukum PDP.

Keywords:
BPJS Kesehatan, Personal Data, Data Breach, Corporation, PDP Law.

ABSTRACT

Insiden kebocoran data peserta BPJS Kesehatan pada 2021 memperlihatkan rapuhnya keamanan informasi di Indonesia. Peristiwa tersebut memperlihatkan bagaimana jutaan data penduduk beredar di forum daring dan menimbulkan kekhawatiran publik terkait perlindungan privasi. Situasi ini menegaskan urgensi regulasi yang mengatur perlindungan data pribadi. UU No. 27 Tahun 2022 disahkan untuk memberi kepastian hukum bagi subjek data dan menetapkan kewajiban bagi pengendali data, termasuk BPJS Kesehatan yang mengelola data berskala nasional. Penelitian ini bertujuan menguraikan tanggung jawab hukum BPJS Kesehatan sebagai korporasi publik dalam mengelola data peserta, serta menilai implikasi hukum apabila terjadi kelalaian yang berujung kebocoran. Pendekatan yang digunakan ialah penelitian hukum normatif melalui analisis aturan perundang-undangan dan literatur ilmiah. Hasil penelitian memperlihatkan bahwa BPJS Kesehatan memikul tanggung jawab signifikan sebagai pengendali data berdasarkan UU PDP, yang mencakup kewajiban keamanan, transparansi, serta pengelolaan data sesuai prinsip perlindungan data pribadi. Kasus kebocoran tahun 2021 memperlihatkan lemahnya tata kelola keamanan digital yang berdampak terhadap reputasi lembaga serta potensi pertanggungjawaban hukum. UU PDP merumuskan konsekuensi administratif, perdata, dan pidana bagi pengendali data yang lalai. Diperlukan penguatan keamanan, kepatuhan, dan audit internal untuk mencegah insiden berulang.

The massive data breach involving BPJS Kesehatan in 2021 revealed the vulnerability of Indonesia's digital security ecosystem. Millions of citizens' personal data appeared on online forums, raising concerns regarding privacy protection and institutional accountability. This incident underscored the urgent need for a comprehensive regulatory framework governing personal data protection. Law No. 27 of 2022 establishes clear obligations for data controllers and affirms the rights of data subjects, including individuals whose information is processed by public institutions such as BPJS Kesehatan. This study examines the legal responsibilities of BPJS Kesehatan as a public corporation in managing participants' personal data, and explores the legal implications arising from negligence that results in data breaches. A normative legal approach is applied through statutory analysis and examination of academic literature. Findings show that BPJS Kesehatan bears substantial obligations as a data controller under the Personal Data Protection Law, including ensuring data security, maintaining transparency, and implementing proper data governance mechanisms. The 2021 breach demonstrated significant gaps in digital security infrastructure that affected public trust and exposed potential legal liabilities. The PDP Law provides administrative, civil, and criminal consequences for violations committed by data controllers. Strengthening of security, compliance, and internal audits is necessary to prevent recurrence of incidents.

How to Cite: Ridho Rivantoro, et al (2025), Tanggung Jawab Hukum Korporasi Atas Kebocoran Data Peserta BPJS Kesehatan Berdasarkan UU No. 27 Tahun 2022, 4(3). https://doi.org/10.31004/jerkin.v4i3.4575

PENDAHULUAN

Perkembangan teknologi digital memperluas pola pemanfaatan data pribadi dalam layanan publik. Kondisi tersebut menghadirkan potensi risiko apabila pengendali data tidak menerapkan standar keamanan yang kuat (Nasution, 2021). Situasi ini tampak dalam kasus kebocoran data peserta BPJS Kesehatan pada 2021, ketika ratusan juta data penduduk muncul dalam forum daring yang menawarkan data tersebut kepada publik. Informasi yang beredar mencakup identitas dasar yang bersifat sensitif dan berpengaruh terhadap keamanan pribadi warga negara. Pemerintah merespons situasi ini melalui investigasi serta pemblokiran situs yang memperjualbelikan data tersebut (CNBC Indonesia, 2021a, 2021b; Detik.com, 2021)

Kasus tersebut menyoroti lemahnya perlindungan data di sektor publik. BPJS Kesehatan menjadi perhatian utama karena kedudukannya sebagai lembaga pengelola data besar yang menyimpan informasi jutaan peserta. Kebocoran ini memunculkan kekhawatiran publik serta pertanyaan mengenai tanggung jawab hukum korporasi publik dalam mengelola data pribadi. Kondisi tersebut mempertegas kebutuhan landasan hukum komprehensif dalam perlindungan data pribadi, yang kemudian diwujudkan melalui UU No. 27 Tahun 2022 (Pemerintah Republik Indonesia, 2022).

Kajian akademik memperlihatkan bahwa regulasi sebelumnya belum memberi kepastian terkait tanggung jawab badan hukum publik dalam kasus pelanggaran data (Saly et al., 2023). Padahal lembaga seperti BPJS memikul amanat konstitusional dalam memberikan layanan publik yang mengandalkan kepercayaan peserta. Ketika data tersebut tidak dikelola secara aman, kepercayaan publik dapat terganggu dan memberi dampak hukum bagi lembaga pengelola data (Pase, 2025).

Penelitian sebelumnya lebih sering membahas isu kebocoran data dari sisi keamanan informatika atau pertanggungjawaban pidana secara umum (Nugraha et al., 2025; Maulida & Utomo, 2023). Kajian yang menempatkan BPJS sebagai korporasi publik yang mempunyai tanggung jawab hukum menyeluruh masih terbatas. Situasi ini menghadirkan ruang penelitian yang penting untuk memahami tanggung jawab tersebut berdasarkan kerangka UU PDP.

Penelitian ini bertujuan menguraikan bagaimana tanggung jawab hukum BPJS sebagai pengendali data serta implikasi hukum yang dapat timbul apabila terjadi kelalaian. Analisis difokuskan pada keterkaitan antara prinsip perlindungan data pribadi dan kewajiban institusional sebagaimana termuat dalam UU PDP. Kajian ini menghadirkan gambaran mengenai penguatan regulasi serta praktik tata kelola data di lembaga publik.

Untuk menjawab penelitian ini, penelitian difokuskan pada dua rumusan masalah, yaitu (1) Bagaimana kedudukan BPJS Kesehatan sebagai pengendali data? dan (2) Bagaimana tanggung jawab BPJS Kesehatan sebagai pengendali data?

METODE

Penelitian ini menggunakan pendekatan hukum normatif dengan menelaah ketentuan perundang-undangan, literatur ilmiah, dan dokumen resmi terkait perlindungan data pribadi. Sumber data penelitian meliputi bahan hukum primer berupa UU No. 27 Tahun 2022, UU No. 24 Tahun 2011 tentang BPJS, dan regulasi pendukung. Bahan hukum sekunder mencakup buku dan jurnal ilmiah yang memberi landasan teori mengenai perlindungan data pribadi, tanggung jawab hukum, serta aspek teknis pengelolaan data di sektor publik (Gani, 2023; Marzuki, 2017).

Teknik pengumpulan data dilakukan melalui studi dokumen dengan menelaah seluruh peraturan dan literatur yang relevan. Analisis data dilakukan melalui pendekatan deskriptif-analitis dengan menafsirkan norma hukum serta menghubungkannya dengan kasus kebocoran data BPJS. Kerangka teori yang digunakan meliputi teori tanggung jawab hukum (Solove, 2022) dan teori perlindungan data pribadi yang menempatkan hak subjek data sebagai perhatian utama kebijakan privasi.

HASIL DAN PEMBAHASAN

Kedudukan BPJS Kesehatan sebagai Pengendali Data

BPJS Kesehatan memiliki kedudukan hukum yang kuat sebagai badan hukum publik yang dibentuk berdasarkan amanat UU No. 24/2011. Status tersebut memberikan legitimasi bagi BPJS untuk mengelola data peserta dalam lingkup nasional sekaligus menempatkannya sebagai institusi yang memegang tanggung jawab besar terhadap informasi kesehatan dan identitas warga negara. Pengaturan

ini mempertegas bahwa setiap instrumen teknis maupun administratif yang digunakan dalam proses pendataan harus mengacu pada standar kelembagaan yang telah ditetapkan oleh regulasi. Kehadiran BPJS sebagai pengelola data resmi menuntut adanya sistem yang mapan, mekanisme penyimpanan yang terstruktur, serta prosedur kerja yang menjamin keamanan informasi peserta.

Kewenangan yang dimiliki BPJS Kesehatan menciptakan tuntutan agar setiap proses pengumpulan, penyimpanan, dan pemanfaatan data dilakukan secara cermat sesuai ketentuan hukum. Pengelolaan data dalam konteks lembaga publik memerlukan kepatuhan terhadap prinsip integritas dan akuntabilitas demi menjaga kejelasan alur pertanggungjawaban. Proses tersebut mencakup pengaturan internal yang mengontrol akses, penggunaan teknologi yang aman, serta penerapan tata kelola yang selaras dengan pedoman perlindungan data. Setiap langkah operasional harus dirancang untuk meminimalkan potensi penyimpangan dan memastikan seluruh pemrosesan informasi dapat diaudit dengan jelas oleh otoritas pengawas maupun masyarakat.

Data peserta yang dihimpun BPJS mencerminkan identitas personal dan hak dasar warga negara sehingga pengelolaannya memerlukan tingkat kehati-hatian yang tinggi. Informasi tersebut berkaitan dengan aspek penting dalam kehidupan publik, sehingga lembaga pengelola wajib memegang komitmen kuat terhadap prinsip legalitas dalam menjalankan mandatnya. Mekanisme pengolahan data harus diarahkan untuk menjaga kerahasiaan, keakuratan, dan perlindungan ruang privat warga. Ketaatan terhadap regulasi menjadi fondasi utama agar pengelolaan data memberikan rasa aman, memperkuat kepercayaan masyarakat, serta memastikan bahwa penyelenggaraan program jaminan sosial berjalan sesuai tujuan hukum yang mendasarinya.

UU PDP Pemerintah Republik Indonesia (2022) menegaskan bahwa pengendali data wajib menjaga keakuratan, keamanan, serta pengelolaan data yang bersandar pada persetujuan yang jelas dari pemilik data. BPJS terikat pada prinsip ini karena ruang lingkup pengelolaan datanya bersifat luas dan mencakup hampir seluruh penduduk Indonesia. Pengelolaan yang dimaksud meliputi proses pengumpulan, penyimpanan, penggunaan, dan penyediaan data bagi pihak berwenang. Kewajiban tersebut menuntut struktur pengelolaan yang sistematis agar seluruh tahapan pengolahan berjalan sesuai standar hukum perlindungan data.

Tanggung jawab BPJS sebagai pengendali data terbentang pada bidang administratif dan teknis. Pengamanan sistem, pembatasan akses informasi, hingga penyelenggaraan audit berkala merupakan bentuk kewajiban yang menunjukkan keseriusan lembaga dalam meminimalkan potensi risiko kebocoran. Dalam konteks hukum perlindungan data pribadi, aspek keamanan ini merupakan fondasi penting untuk menjaga kepercayaan peserta sekaligus memastikan sistem informasi berjalan stabil. Fondasi tersebut semakin relevan seiring meningkatnya ancaman peretasan yang menargetkan lembaga publik.

Teori tanggung jawab hukum yang dijelaskan Solove et al., (2023) menempatkan korporasi sebagai entitas yang harus menjamin keamanan informasi yang dikelolanya. Pandangan akademik ini menguatkan kewajiban BPJS selaku lembaga publik yang memiliki wewenang eksklusif atas data peserta. Teori tersebut menegaskan bahwa setiap kelalaian dalam perlindungan data berpotensi menimbulkan tanggung jawab hukum. Konsep ini memperkuat pemahaman bahwa tata kelola keamanan informasi harus diatur melalui mekanisme yang konsisten dan dapat diawasi secara menyeluruh.

Tanggung Jawab Hukum BPJS Berdasarkan UU PDP

Pada Mei 2021 publik dikejutkan dengan kemunculan data peserta BPJS Kesehatan di forum daring yang menawarkan lebih dari 279 juta informasi identitas warga. Data yang beredar mencakup NIK, nama, alamat, hingga status keanggotaan. Pemerintah kemudian melakukan penelusuran dan menemukan kesesuaian signifikan antara data tersebut dan data resmi BPJS (Detik.com, 2021). Peristiwa ini menunjukkan bagaimana kelemahan pada satu titik sistem dapat berdampak luas terhadap keamanan data nasional.

Insiden yang muncul pada tahun 2021 mendorong dilakukannya berbagai kajian akademik yang berfokus pada kelemahan dalam pengelolaan sistem informasi lembaga publik. Peristiwa tersebut membuka perhatian luas mengenai bagaimana struktur pengamanan data di sektor pemerintahan masih menghadapi tantangan besar dalam hal konsistensi penerapan standar keamanan. Para peneliti menilai bahwa kejadian tersebut menunjukkan betapa pentingnya pemetaan risiko sejak tahap perancangan hingga tahap implementasi sistem digital. Situasi ini kemudian menjadi dasar bagi banyak analisis yang

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

menekankan bahwa penguatan arsitektur teknologi informasi perlu dirancang secara berlapis agar potensi akses yang tidak semestinya dapat diminimalisir.

Kajian yang dilakukan oleh Nugraha et al., (2025) mengemukakan bahwa insiden tersebut mengungkap adanya kerentanan yang bersifat struktural dan berakar pada tata kelola sistem yang belum sepenuhnya matang. Kondisi tersebut memungkinkan pihak yang tidak memiliki otorisasi untuk mendapatkan akses terhadap data dalam jumlah besar melalui celah yang muncul akibat kelemahan teknis maupun administratif. Analisis tersebut menegaskan bahwa kesiapan perangkat digital harus disertai pengaturan prosedural yang tegas sehingga setiap proses pemrosesan data berada dalam pengawasan yang memadai. Pemahaman mengenai sumber kerentanan ini sangat penting karena dapat menjadi dasar perbaikan yang lebih menyeluruh dalam pengembangan sistem keamanan institusi publik.

Kerentanan yang dipaparkan dalam berbagai penelitian berkaitan erat dengan kapasitas infrastruktur digital, kualitas kontrol internal, serta ketepatan desain operasional yang digunakan dalam pengelolaan informasi. Kondisi ini menggambarkan bahwa sistem yang belum diperkuat melalui standar keamanan komprehensif berisiko mengalami paparan data dalam bentuk yang sulit dikendalikan. Peristiwa tersebut memberikan gambaran nyata mengenai urgensi peningkatan tata kelola teknologi agar integritas dan kerahasiaan informasi dapat terjamin sepenuhnya. Penguatan kebijakan, peningkatan kompetensi teknis, serta pengawasan berkelanjutan menjadi unsur yang saling berhubungan untuk mencegah terulangnya kejadian serupa pada masa mendatang.

Dalam perspektif hukum, kebocoran ini menunjukkan adanya kegagalan BPJS dalam memastikan perlindungan data sesuai standar yang berlaku bagi pengendali data. Tindakan yang menimbulkan akses ilegal pada data pribadi menjadi dasar munculnya potensi tanggung jawab hukum terhadap lembaga. Kelalaian dalam aspek teknis maupun administratif dapat dipandang sebagai bentuk pengabaian terhadap kewajiban yang telah ditetapkan undang-undang. Pandangan ini mempertegas bahwa pengendali data harus menjaga keamanan sistem secara konsisten.

Peristiwa ini memperlihatkan pentingnya evaluasi menyeluruh pada tata kelola keamanan informasi di lembaga publik. Kasus tersebut mencatat bahwa ancaman dunia digital berkembang cepat sehingga penyesuaian kebijakan keamanan harus dilakukan secara berkelanjutan. Penguatan prosedur operasional, peningkatan kemampuan teknis pegawai, serta pemantauan sistem secara real-time menjadi kebutuhan strategis. Insiden tahun 2021 menjadi pengalaman penting yang menandai perlunya transformasi mendalam dalam manajemen risiko data.

UU PDP memberikan kerangka jelas mengenai kewajiban pengendali data dalam memastikan seluruh tahapan pengolahan berlangsung aman, proporsional, dan transparan. BPJS sebagai pengendali data diharuskan menerapkan langkah pengamanan yang memadai agar informasi peserta terlindungi dari ancaman akses ilegal. Ketentuan ini mencakup mekanisme teknis seperti enkripsi, sistem autentikasi, serta prosedur administratif yang mengatur alur pemrosesan data. Prinsip ini menunjukkan bahwa perlindungan data harus berjalan secara terpadu pada setiap tahap.

Dalam konteks pertanggungjawaban, BPJS dapat dikenai sanksi administratif apabila terbukti lalai menjalankan kewajiban pengamanan. Sanksi tersebut dapat berupa teguran, denda administratif, atau penghentian sementara kegiatan pengolahan data. Konsekuensi ini menunjukkan bahwa UU PDP memiliki instrumen tegas untuk memastikan pengendali data menjalankan kewajiban hukum secara konsisten. Instrumen tersebut berfungsi sebagai mekanisme kontrol guna mencegah terulangnya insiden serupa.

UU PDP juga membuka ruang bagi subjek data untuk mengajukan tuntutan ganti rugi apabila mengalami kerugian akibat kelalaian BPJS. Mekanisme perdata memberi hak kepada individu untuk memperoleh pemulihan atas kerusakan yang timbul dari penyalahgunaan atau kebocoran data pribadi. Proses ini memperlihatkan bahwa pengendali data tidak hanya berhadapan dengan risiko administratif, tetapi juga potensi konsekuensi finansial. Hal ini menegaskan pentingnya pengendali data mengelola risiko secara terukur.

Sanksi pidana dapat dikenakan apabila terdapat tindakan yang mengandung unsur kelalaian berat atau perbuatan melawan hukum dalam pengelolaan data. Penegakan pidana berlaku pada pihak yang secara langsung bertanggung jawab terhadap tindakan tersebut. Ketentuan pidana ini dirancang untuk memberi efek pencegahan pada seluruh pihak yang terlibat dalam pemrosesan data. Ranah pidana memperkuat rezim perlindungan data dengan memastikan bahwa penyimpangan dalam pemrosesan data memiliki konsekuensi hukum yang jelas.

Implikasi Hukum atas Kelalaian Pengendali Data

Teori perlindungan data pribadi memandang bahwa setiap pelanggaran kewajiban dari pengendali data membawa konsekuensi langsung terhadap hak-hak subjek data. (Pinondang & Thalib, 2024) menekankan bahwa setiap individu memiliki hak untuk mengetahui proses pengumpulan informasi, memahami tujuan penggunaannya, serta memastikan bahwa data tersebut memperoleh penjagaan yang memadai. Hak tersebut memberi ruang bagi masyarakat untuk menuntut pertanggungjawaban ketika informasi pribadi mereka diproses tanpa dasar yang sah, digunakan secara keliru, atau mengalami kebocoran yang menimbulkan kerugian.

Posisi ini menegaskan bahwa subjek data merupakan pihak yang rentan terhadap risiko penyalahgunaan informasi sehingga harus ditempatkan sebagai pusat perhatian dalam setiap kebijakan pengelolaan data. Perlindungan yang dimaksud mencakup transparansi dari pihak pengendali data, pengamanan teknis maupun administratif, serta kejelasan mengenai pihak yang berwenang mengakses informasi tersebut. Kerangka pemikiran ini mendorong terbentuknya mekanisme pengawasan yang memastikan bahwa seluruh proses pengolahan data berlangsung sesuai prinsip akuntabilitas dan integritas.

Pandangan tersebut memperkuat pentingnya sistem hukum dan regulasi yang mampu menjamin hak subjek data secara berkelanjutan. Masyarakat memperoleh landasan untuk mengajukan keberatan, meminta klarifikasi, hingga menuntut pemulihan bila terjadi pelanggaran yang merugikan. Upaya ini membangun kesadaran bahwa data pribadi adalah bagian dari identitas seseorang yang harus dijaga secara serius, sekaligus menumbuhkan tanggung jawab bagi setiap pihak yang menjalankan fungsi pengendalian data agar selalu mematuhi standar perlindungan yang berlaku.

Insiden kebocoran yang terjadi memperlihatkan bahwa lemahnya tata kelola keamanan dapat menimbulkan ancaman besar terhadap privasi publik. Dalam beberapa kajian, faktor seperti literasi keamanan digital yang rendah, keterbatasan audit, serta minimnya pengawasan internal disebut sebagai pemicu utama terjadinya kebocoran (Annan, 2024; Rinjani & Firmansyah, 2025). Situasi ini menunjukkan perlunya penguatan mekanisme pengawasan yang mampu memantau sistem secara menyeluruh. Pengawasan yang kuat dapat menekan risiko terjadinya pelanggaran.

Implikasi hukum bagi pengendali data yang lalai tidak berhenti pada aspek sanksi, sebab kelalaian juga mengakibatkan hilangnya kepercayaan masyarakat. Kepercayaan publik merupakan komponen penting dalam penyelenggaraan layanan berbasis data karena sistem jaminan sosial sangat bergantung pada partisipasi peserta. Ketika kepercayaan menurun, kualitas hubungan antara lembaga publik dan masyarakat ikut terdampak. Kondisi tersebut menunjukkan bahwa pemulihan sistem harus disertai pemulihan kepercayaan publik.

Reformulasi tata kelola keamanan data menjadi kebutuhan jangka panjang bagi lembaga publik. Pembaruan sistem, peningkatan kapasitas sumber daya manusia, serta penyusunan regulasi internal yang lebih ketat menjadi langkah strategis untuk memperkuat perlindungan data. Reformulasi ini bertujuan menciptakan lingkungan pengelolaan data yang lebih kuat serta mampu menyesuaikan diri dengan perkembangan ancaman digital. Kajian akademik menegaskan bahwa perbaikan yang dilakukan secara berkelanjutan akan memberikan fondasi yang lebih stabil bagi keamanan informasi nasional.

SIMPULAN

BPJS Kesehatan memiliki posisi sebagai pengendali data yang memikul kewajiban hukum dalam menyusun pengelolaan informasi peserta secara aman. Insiden kebocoran data pada 2021 memperlihatkan bahwa sistem keamanan yang tersedia belum memenuhi standar perlindungan yang diatur dalam UU No. 27 Tahun 2022. Situasi tersebut menimbulkan risiko terhadap hak subjek data dan menunjukkan perlunya penerapan prinsip perlindungan data yang lebih kuat. Kewajiban pengendali data mencakup aspek teknis, administratif, dan prosedural, yang harus dijalankan untuk memastikan bahwa informasi peserta berada dalam kondisi yang terlindungi.

Upaya penegakan tanggung jawab hukum terhadap pengendali data telah diatur melalui ketentuan administratif, perdata, serta pidana sesuai UU PDP. Ketentuan tersebut memberi ruang bagi subjek data untuk menuntut ganti rugi apabila terjadi kelalaian yang menimbulkan kerugian. Hasil penelitian menunjukkan perlunya peningkatan kepatuhan normatif, penguatan infrastruktur keamanan digital, serta pengawasan internal yang konsisten di lingkungan BPJS Kesehatan. Penerapan langkah-langkah

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

tersebut diharapkan dapat mendukung keberlanjutan tata kelola data yang lebih aman dan meningkatkan kepercayaan masyarakat terhadap layanan publik.

BPJS Kesehatan, dalam kedudukannya sebagai pengendali data, disarankan untuk memperkuat tata kelola perlindungan data pribadi melalui peningkatan standar keamanan teknis dan administratif yang lebih komprehensif. Penguatan ini harus difokuskan pada pembaruan arsitektur keamanan siber yang mencakup penerapan enkripsi data tingkat lanjut, pembatasan hak akses yang ketat, serta pelaksanaan audit sistem informasi secara berkala. Langkah ini diperlukan untuk memastikan bahwa seluruh prosedur pengumpulan, penyimpanan, dan pemrosesan data peserta benar-benar mematuhi prinsip integritas dan kerahasiaan sebagaimana diamanatkan oleh regulasi, sekaligus meminimalkan celah kerentanan yang dapat dimanfaatkan oleh pihak tidak berwenang.

Selanjutnya, guna memitigasi risiko pertanggungjawaban hukum akibat kelalaian atau kebocoran data, BPJS Kesehatan perlu menyusun manajemen risiko yang lebih proaktif serta mekanisme pemulihan yang transparan bagi subjek data. Hal ini dapat diwujudkan melalui peningkatan kompetensi sumber daya manusia di bidang keamanan digital, penerapan sistem pemantauan ancaman secara real-time, serta penyediaan saluran pengaduan yang responsif untuk menangani keluhan masyarakat. Upaya preventif dan responsif ini sangat krusial tidak hanya untuk menghindarkan lembaga dari sanksi administratif, perdata, maupun pidana sesuai UU PDP, tetapi juga sebagai langkah strategis untuk memulihkan dan menjaga kepercayaan publik terhadap integritas penyelenggaraan jaminan sosial nasional.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah berkontribusi dalam pelaksanaan penelitian sekaligus penyusunan artikel ini.

REFERENSI

Aditya Nugraha, D., Nurfitroh, R., Dhiya Ul-Haq, N., Purnama Dika, R., Novebriana Lagontang, S., Studi Teknik Informatika, P., & Tinggi Teknologi Wastukancana, S. (2025). KEBOCORAN DATA BPJS KESEHATAN: ANCAMAN TERHADAP KEAMANAN INFORMASI PUBLIK DI ERA DIGITAL. *Integrative Perspectives of Social and Science Journal*, *2*(3), 4685.

Annan, A. (2024). Tinjauan yuridis perlindungan data pribadi pada sektor kesehatan berdasarkan UU No. 27 Tahun 2022. *SYNERGI Jurnal Ilmiah Multidisiplin*, *1*(4), 247. https://e-journal.naureendigition.com/index.php/sjim

CNBC Indonesia. (2021a, May 21). *Kominfo blokir situs yang jual data diduga milik BPJS*. Https://Www.Cnnindonesia.Com/Teknologi/20210521123238-185-646963/Kominfo-Blokir-Situs-Yang-Jual-Data-Diduga-Milik-Bpjs.

CNBC Indonesia. (2021b, May 23). *Heboh! Situs klaim jual 279 juta data penduduk RI*. Https://Www.Cnbcindonesia.Com/Tech/20210523092159-37-247634/Heboh-Situs-Klaim-Jual-279-Juta-Data-Penduduk-Ri.

Detik.com. (2021, May 22). *Kominfo: Data pribadi WNI yang bocor identik data BPJS Kesehatan*. Https://News.Detik.Com/Berita/d-5577462/Kominfo-Data-Pribadi-Wni-Yang-Bocor-Identik-Data-Bpjs-Kesehatan.

Gani, T. A. (2023). *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press.

Marzuki, P. M. (2017). *Penelitian Hukum*. Kencana Prenada Media.

Maulida, O., & Utomo, H. (2023). Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna dalam Perspektif Hukum Pidana. *Indonesian Journal of Law and Justice*, *1*(2), 10. https://doi.org/10.47134/ijlj.v1i2.2011

Nasution, A. (2021). *Perlindungan Data Pribadi Di Era Digital*. RajaGrafindo Persada.

Pase, A. T. (2025). Civil Liability In Business Contract Disputes: Implications For Investor Confidence Tanggung Jawab Perdata Dalam Sengketa Kontrak Bisnis: Implikasi Terhadap Kepercayaan Investor. In *Jurnal Hukum Sehasen* (Vol. 11, Issue 1).

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

Pinondang, E. A. M., & Thalib, E. F. (2024). Tinjauan yuridis perlindungan data pribadi dalam tindakan doxing berdasarkan UU Nomor 27 Tahun 2022. *Jurnal Darma Agung*, *32*(5), 421–433.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). 4.+064P-Jeane+Neltje-Revisi.docx. *Jurnal Serina Sosia Humaniora*, *3*, 145.

Solove, D. J., Marshall, J., Research, H., & Washington, G. (2023). The Limitations of Privacy Rights. *Note Dame Law Review*, 975–1036. https://scholarship.law.nd.edu/ndlr

ISSN 2963-7856 (print), ISSN 2961-9890 (online)