SANKSI 2026
Seminar Nasional Hukum, Sosial dan Ekonomi

E-ISSN: 2828-3910

KEBIJAKAN DALAM MENGATASI DAN MELINDUNGI KEBOCORAN DATA NASABAH ASURANSI JIWA ERA LITERASI DIGITAL DI INDONESIA

Chairuni Nasution, Adi Mansar, Faisal

Universitas Muhammadiyah Sumatera Utara
Email: chairuninst@gmail.com (Corresponding Auhtor)

ABSTRAK

Kemajuan teknologi informasi terutama dalam bidang interkoneksi jaringan memberikan pengaruh yang sangat signifikan terhadap berbagai aspek kehidupan manusia yang memberikan dampak signifikan pada ekonomi, sosial dan budaya. Seiring dengan semakin meluasnya penggunaan internet, maka perlindungan data pribadi nasabah asuransi jiwa dari kebocoran data semakin mengkhawatirkan. Data pribadi kini menjadi aset yang sangat berharga dan rentan terhadap berbagai ancaman, seperti peretasan, pencurian identitas serta penyalahgunaan informasi. Penelitian ini menggunakan jenis penelitian hukum normatif (yuridis normatif) dengan pendekatan perundang-undangan (*statute approach*), pendekatan filsafat (*philosophical approach*) serta pendekatan konseptual (*conceptual approach*). Adapun metode penelitiannya kepustakaan (*library research*). Perusahaan asuransi memegang data paling sensitif, seperti kesehatan, keuangan serta identitas yang menjadi target utama bagi pelaku untuk melakukan tindak kejahatannya dengan cara membocorkan data nasabahnya. Rendahnya literasi digital & sosial engineering. Pelaku sering mengeksploitasi kelengahan nasabah (*human error*) akibat literasi digital yang belum merata sebagai dampak kelemahan sistem yang masih belum terkontrol. Tantangan urgensi regulasi sebagaimana diatur dalam Undang-Undang RI Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), implementasi pengawasan dan penegakan hukum masih dalam tahap awal sehingga kompleksitas pihak ketiga dalam hubungan kerjasama dengan *fintech* atau *cloud computing* semakin menambah kerentanan kebocoran data. Kebijakan yang ada masih memerlukan aturan turunan yang spesifik untuk sektor asuransi guna mengisi kesenjangan kewenangan dan pengawasan langsung oleh pihak Otoritas Jasa Keuangan (OJK) terhadap keamanan data digital.

Kata Kunci: Kebocoran Data, Asuransi Jiwa, Literasi Digital.

PENDAHULUAN

A. Latar Belakang

Secara global internet mengalami perkembangan yang sangat pesat, dimana peranannya sangat penting di masyarakat yang ditandai dengan mudahnya akses informasi, percepatan komunikasi dan askes lain yang menggunakan sarana internet. Salah satu sektor yang terpengaruh adalah sektor perbankan, keuangan, investasi, penanaman modal, pasar modal dan perusahaan, termasuk salah satunya perusahaan yang bergerak di bidang asuransi yang memobilisasi dana masyarakat. Teknologi informasi

E-ISSN: 2828-3910

dan komunikasi telah melahirkan inovasi serta memberikan dampak efisien dan ektivitas yang luar biasa.[1]

E-banking adalah layanan yang memungkinkan nasabah perusahaan asuransi jiwa memperoleh informasi, berkomunikasi dan melakukan transaksi melalui sarana elektronik, seperti : ATM, *phone banking*, transfer dana elektronik. Undang-Undang Dasar RI Tahun 1945 sebagai landasan Kostitusional, Pasal 28G ayat (1) menegaskan bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".[2]

Hal ini menjadi dasar konstitusional terhadap perlindungan privasi dan keamanan data pribadi sebagai bagian dari perlindungan diri.[3] Selanjutnya Pasal 28J ayat (1) yang menyebutkan juga bahwa "Setiap orang wajib menghormati hak asasi manusia orang lain dalam tertib kehidupan bermasyarakat, berbangsa, dan bernegara". Merupakan dasar pembatasan dan kewajiban korporasi/individu agar tidak melanggar privasi serta keamanan data pihak lain.[4]

Pasal 246 Kitab Undang- Undang Hukum Dagang (disingkat dengan KUHD) disebut bahwa "Asuransi atau pertanggungan adalah suatu perjanjian dengan mana seorang penanggung mengikatkan diri kepada seseorang tertanggung, dengan menerima suatu premi, untuk memberikan penggantian kepadanya karena suatu kerugian, kerusakan atau kehilangan keuntungan yang diharapkan, yang mungkin akan diderita karena suatu peristiwa yang tan tertentu."

Berdasarkan BAB I Pasal 1 ayat (1) Undang-Undang Republik Indonesia Nomor 40 Tahun 2014 tentang Perasuransi. Pengertian Asuransi adalah "Perjanjian antara dua pihak, yaitu perusahaan asuransi dan pemegang polis, yang menjadi dasar bagi penerimaan premi oleh perusahaan asuransi sebagai imbalan untuk : *Pertama*, memberikan penggantian kepada tertanggung atau pemegang polis karena kerugian, kerusakan, biaya yang timbul, kehilangan keuntungan, atau tanggung jawab hukum kepada pihak ketiga yang mungkin diderita tertanggung atau pemegang polis karena terjadinya suatu peristiwa yang tidak pasti; atau;

Kedua, memberikan pembayaran yang didasarkan pada meninggalnya tertanggung atau pembayaran yang didasarkan pada hidupnya tertanggung dengan manfaat yang besarnya telah ditetapkan dan/atau didasarkan pada hasil pengelolaan dana. Di Indonesia pengaturan yuridis terhadap kejahatan siber diatur dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat dengan UU ITE), UndangUndang Republik Indonesia Nomor

[1] Resa Raditio, *Aspek Hukum Transaksi Elektronik*, Graha Ilmu, Jakarta, 2014, hlm. 65

[2] Mulyati, *Aspek Perlindungan Hukum Atas Data Pribadi Nasabah Pada Penyelenggaraan Layanan Internet Banking*, Fakultas Syariah dan Hukum, UIN AR-RANIRY Darussalam, Aceh, 2017, hlm. 40

[3] Jimly Asshiddiqie dan Hafid Abbas, *Hak Asasi Manusia Dalam Konstitusi Indonesia Dari UUD 1945 Sampai dengan Perubahan UUD 1945 Tahun 2002*, Edisi Kelima, Prenada Media, Group, Jakarta, 2010, hlm. 8

[4] Miriam Budiardjo, *Pembangunan Politik, Situasi Global dan Hak Asasi Di Indonesia*, Gramedia, Jakarta, 1994, hlm. 45

E-ISSN: 2828-3910

19 Tahun 2016 dan Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 merupakan perubahan atas Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 yang menjadi landasan hukum di Negara Kesatuan Republik Indodesia (NKRI) dalam beraktivitas di dunia mayantara.[5]

Undang-undang ini telah melengkapi hukum pidana materiil yang mengatur berbagai tindak pidana yang berkembang seiring dengan pertumbuhan teknologi informasi dan komunikasi.[6] Asuransi digital merupakan suatu produk yang dikembangkan oleh perusahaan asuransi dengan mengikuti perkembangan teknologi saat ini. Pengawasan terhadap data pribadi pada asuransi digital dilakukan oleh pihak perusahaan asuransi sedangkan pihak Otoritas Jasa Keuangan (OJK) hanya melakukan pengawasan terhadap kegiatan usaha perusahaan asuransinya.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sehingga kedepannya diharapkan undang-undang tersebut dapat memberikan perlindungan hukum terhadap subjek data pribadi.

Tindakan awal tersebut sangatlah penting mengingat pengungkapan data pribadi tanpa kendali dapat menimbulkan banyak risiko terhadap subjek data pribadi serta organisasi serta meningkatkan kemungkinan tindak kriminalitas, mulai dari ancaman, perundungan, penipuan hingga pembobolan akun yang dimiliki oleh subjek data pribadi. Perusahaan asuransi saat ini telah mengikuti perkembangan teknologi.

Wujud dari berkembangnya teknologi digital memungkinkan orang untuk dapat memperoleh informasi secara cepat dan akurat, hal ini tentu saja dimanfaatkan oleh pihak yang berkepentingan yang salah satunya adalah pihak pengelolaan jasa keuangan dalam hal ini perusahaan asuransi dengan melakukan terobosan yaitu membuat asuransi digital.

B. Rumusan Masalah

Permasalahan dalam kajian ini dibatasi dalam rumusan masalah, yaitu sebagai berikut:

1. Bagaimana kebijakan dalam mengatasi kebocoran data nasabah asuransi jiwa era literasi digital?
2. Bagaimana kebijakan dalam melindungi privasi data nasabah asuransi jiwa dari kebocoran data era literasi digital saat ini?

C. Metode Penelitian

Penelitian ini menggunakan penelitian hukum normatif (yuridis normatif). Menurut pendapat Soerjono Soekanto dan Sri Mamudji mengatakan bahwa penelitian hokum normatif atau penelitian hukum kepustakaan adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka.[7]

---

[5] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung, 2012, hlm. 213

[6] Nudirman Munir, *Pengantar Hukum Siber Indonesia*, Edisi Ketiga, Rajawali Perss, Jakarta, 2017, hlm. 76

[7] Ramlan, *Metode Penelitian Hukum Dalam Pembuatan Karya Ilmiah*, Cetakan Pertama, UMSU PRESS, Medan, 2023, hlm. 68

E-ISSN: 2828-3910

HASIL DAN PEMBAHASAN

1. Kebijakan Dalam Mengatasi Kebocoran Data Nasabah Asuransi Jiwa Era Literasi Digital

Kelemahan sistem keamanan kerentanan perangkat lunak, kelemahan dalam konfigurasi sistem dan keamanan jaringan yang tidak memadai sering menjadi penyebab utama kebocoran data. kesalahan manusia (*human error*), seperti pengiriman email ke penerima yang salah atau pengelolaan password yang buruk, juga penyebab signifikan kebocoran data. Serangan siber, seperti *phishing, malware, ransomware*, dan *hacking* dapat menyebabkan kebocoran data dengan mengeksploitasi celah keamanan.[8]

Kebocoran data dapat menyebabkan kerugian finansial langsung melalui denda, biaya pemulihan, dan kehilangan pendapatan akibat reputasi yang rusak. Reputasi perusahaan atau individu dapat terganggu secara signifikan setelah kebocoran data, yang dapat mengakibatkan kehilangan kepercayaan dari pihak nasabah asuransi jiwa.

Implikasi hukum terhadap pelanggaran peraturan perlindungan data menyebabkan tindakan hukum dan denda yang berat. Beberapa standar industri seperti PCI-DSS untuk data kartu kredit, yang menetapkan praktik terbaik dalam perlindungan data. Penggunaan teknologi keamanan enkripsi dapat melindungi data dengan mengenkripsi informasi sensitif sehingga hanya pihak yang berwenang yang dapat mengaksesnya. *Firewall* dan sistem deteksi intrusi dapat mencegah akses tidak sah dan memantau aktivitas jaringan untuk deteksi dini potensi ancaman. Antivirus dan anti- *malware* dapat menjaga sistem dari infeksi yang dapat menyebabkan kebocoran data.[9]

Kebijakan dan prosedur keamanan terhadap akses kontrol bertujuan menetapkan siapa yang memiliki akses ke data dan bagaimana data tersebut harus diakses dan dikelola. Pelatihan kepada setiap agen di perusahaan asuransi bertujuan memberikan pelatihan keamanan untuk mengenali dan menghindari potensi risiko, seperti : serangan phishing. Pemantauan dan audit, yakni dengan melakukan audit keamanan secara rutin untuk mengidentifikasi potensi kerentanan.

Pemantauan *real-time*, yakni dengan menggunakan alat pemantauan untuk mendeteksi aktivitas yang mencurigakan. Penyusunan rencana dengan menyusun rencana respons insiden yang jelas dan terstruktur untuk menangani kebocoran data serta melakukan tindakan tanggap darurat dengan langkah-langkah seperti isolasi data yang bocor, pemberitahuan kepada pihak yang terdampak dan koordinasi dengan pihak berwenang.

Penilaian dampak analisis kerusakan dengan menilai dampak dari kebocoran data untuk memahami skala dan potensi kerugian. Membuat laporan insiden secara detail untuk dokumentasi dan perbaikan di masa depan. Perbaikan dan peningkatan keamanan terhadap tindakan perbaikan dengan mengidentifikasi dan memperbaiki kerentanan yang menyebabkan kebocoran. Peningkatan prosedur menyempurnakan kebijakan dan prosedur keamanan mematuhi regulasi perlindungan data serta memastikan kepatuhan terhadap regulasi yang berlaku terkait perlindungan data dan melaksanakan langkah-langkah yang diatur.

Strategi pencegahan kebocoran data melalui enkripsi data bertjuan melindungi data sensitif dengan enkripsi saat penyimpanan dan pengiriman. Kontrol akses: menerapkan

---

[8] Mohamad Soleh, *Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital*, Journal of Government, Social and Politics, Volume 11 Number 1 Maret 2024

[9] Lee, S. M & Lee, K. H*, Exploring The Impact Of Data Breaches On Firm Performance And Market Reactions*, Journal of Business Ethics, 176(4), 2022

prinsip *least privilege* untuk membatasi akses hanya kepada yang memerlukan.[10] Monitoring yakni dengan melakukan monitoring secara rutin dan memantau aktivitas jaringan untuk mendeteksi anomali. Pembaruan perangkat lunak secara teratur memperbarui perangkat lunak dan sistem untuk menutup celah keamanan. Kebijakan keamanan data, yakni menyusun dan menegakkan kebijakan yang jelas mengenai pengelolaan data. Rencana Strategi-strategi tersebut di atas dapat membantu meminimalisir risiko kebocoran data. Mitigasi dalam konteks kebocoran data melibatkan langkah-langkah yang diambil untuk mengurangi dampak insiden dan mencegah kerusakan lebih lanjut. Beberapa langkah mitigasi yang penting meliputi :18 a). memutuskan akses, yakni segera menghapus akses pengguna yang terlibat dalam kebocoran untuk menghentikan penyebaran lebih lanjut, b). isolasi sistem terdampak dengan mengisolasi sistem atau jaringan yang terpengaruh untuk mencegah penyebaran kebocoran, c). penerapan patch dan pembaruan, yakni menerapkan patch keamanan untuk menutup celah yang dimanfaatkan dalam serangan, d). perbaikan konfigurasi: menyusun kembali konfigurasi sistem untuk menghilangkan kerentanan, e). komunikasi dengan pemangku kepentingan, yakni memberitahu pihak-pihak terkait tentang insiden dan langkah-langkah yang diambil untuk mengatasi masalah, f). monitoring pasca insiden, yakni memantau aktivitas sistem setelah insiden untuk mendeteksi adanya upaya serangan lebih lanjut.

Pemulihan setelah kebocoran data melibatkan langkah-langkah untuk mengembalikan sistem dan data ke kondisi normal serta memastikan bahwa insiden tidak terulang. Langkah-langkah penting dalam pemulihan meliputi sebagai berikut Restorasi sistem adalah mengembalikan sistem ke versi yang aman, baik melalui backup atau konfigurasi yang telah diuji; Verifikasi keamanan dengan melakukan audit untuk memastikan bahwa semua celah yang menyebabkan kebocoran telah diperbaiki; Pengujian fungsionalitas, yakni dengan memastikan semua sistem berfungsi dengan baik setelah perbaikan dilakukan; Komunikasi dengan pengguna bertujuan memberikan informasi kepada pengguna mengenai langkah- langkah yang diambil untuk memperbaiki situasi dan melindungi data nasabah asuransi jiwa; Penyusunan laporan insiden dengan menyusun laporan menyeluruh tentang insiden, termasuk penyebab, dampak dan langkah-langkah yang diambil untuk mitigasi dan pemulihan serta Tindakan preventif melalui pengimplementasian kebijakan dan prosedur baru untuk mencegah tidak terulangnya kembali kasus-kasus kebocoran privasi data nasabah asuransi jiwa.

Tindak lanjut dari kebocoran data melibatkan evaluasi dan perbaikan system serta kebijakan yang ada. Langkah-langkah yang perlu diambil termasuk: evaluasi insiden, yakni menganalisis secara mendalam tentang penyebab kebocoran dan efektivitas respons yang diambil.

2. Kebijakan Dalam Melindungi Privasi Data Nasabah Asuransi Jiwa Dari Kebocoran Data Era Literasi Digital Saat Ini

Kelemahan dalam sistem perlindungan data tidak semata- mata berasal dari faktor teknis, melainkan disebabkan oleh kurangnya kesadaran akan pentingnya menjaga privasi, baik di lingkungan masyarakat, korporasi, organisasi atau perhimpunan. Hal ini berarti bahwa permasalahan perlindungan data pribadi bukan hanya soal kurangnya teknologi atau sistem keamanan. Akan tetapi, karena banyak masyarakat, korporasi,

[10] Payment Card Industry Data Security Standard (PCI DSS), *PCI DSS Requirements and Security Assessment Procedures*, Retrieved from https://www.pcisecuritystandards.org/document library, 2022

E-ISSN: 2828-3910

organisasi atau perhimpuanaan belum memiliki kebiasaan atau kesadaran untuk menjaga privasi dengan baik. Misalnya, individu sering membagikan data pribadi tanpa pikir panjang dan banyak pihak korporasi (perusahaan asuransi) belum menerapkan aturan atau pelatihan yang cukup untuk melindungi data. Dengan demikian, perlindungan data memerlukan perubahan perilaku dan pola pikir, bukan hanya pembaharuan teknologi saja.[11]

Keamanan informasi adalah langkah untuk melindungi data digital dari kerusakan, pencurian atau akses yang tidak sah. Privasi digital adalah hak masing-masing orang untukmengatur penggunaan data pribadinya di internet. Keduanya saling berhubungan dan menjadi dasar penting dalam mempertahankan keamanan di dunia digital. Kerahasiaan atas privasi identitas atau data nasabah asuransi jiwa memastikan bahwa informasi hanya dapat diakses oleh pihak yang berhak. Integritas menjamin bahwa informasi tidak mengalami perubahan tanpa persetujuan. Ketersediaan: memastikan bahwa informasi selalu dapat diakses saat diperlukan.

Privasi bukan hanya tentang menyembunyikan informasi pribadi agar tidak diketahui orang lain, tetapi lebih kepada bagaimana seseorang memiliki kendali atas penggunaan dan penyebaran data tersebut. Artinya, setiap individu berhak menentukan siapa yang boleh mengakses datanya, untuk tujuan apa, dan sejauh mana data tersebut boleh dibagikan.

Dalam konteks digital saat ini sangat penting karena data pribadi dapat dengan mudah dikumpulkan, dianalisis bahkan diperjualbelikan tanpa sepengetahuan pemiliknya. Oleh karena itu, perlindungan privasi mencakup hak untuk mengetahui, mengatur dan membatasi apa yang terjadi terhadap informasi pribadi seseorang di ruang digital. Solusi dan strategi dalam mengambil langkah kebijakan melindungi privasi identitas dan data nasabah asuransi jiwa dibutuhkan implementasi keamanan sistem secara komprehensif (firewall, anti virus dan pembaharuan sistem). Pendidikan literasi digital bagi masyarakat.

Keamanan informasi dan privasi *online* merupakan hal yang sangat krusial di dunia saat ini. Pemahaman masyarakat mengenai pentingnya menjaga identitas atau data pribadi harus terus diperkuat lewat pendidikan, peraturan dan implementasi teknologi perlindungan. Melaksanakan prinsip kerahasiaan, integritas dan ketersediaan, serta penerapan enkripsi dan pendidikan digital sebagai langkah strategis dalam menciptakan budaya literasi digital keamanan informasi pribadi saat ini.

Sementara itu, regulasi yang ada belum mampu beradaptasi dengan laju perkembangan teknologi seperti : AI, *big data*, dan I*nternet of Things* (IoT)[25], sehingga perlu dilakukan penyesuaian secara terus-menerus agar perlindungan data tetap optimal di tengah tantangan digital yang terus berkembang. Penyelenggara layanan asuransi digital juga harus menyampaikan batasan pemanfaatan data dan informasi kepada pengguna. Perusahaan juga wajib menyampaikan kepada pengguna layanan setiap perubahan tujuan pemanfaatan data dan informasi kepada pengguna dalam hal terdapat perubahan tujuan pemanfaatan data dan informasi.

Untuk melakukan pengawasan secara langsung terhadap data nasabah asuransi secara digital, sehingga apabila terjadi suatu penyelewengan data pribadi nasabah, maka pihak OJK secara langsung mengetahui hal tersebut, sehingga dapat dilakukan suatu

[11] Fitriani, E & Nurhadi, W, *Perlindungan Data Pribadi di Era Digital: Studi Kasus Indonesia*, PT. Refika Utama, Bandung, 2021, hlm. 46

E-ISSN: 2828-3910

tindakan terhadap pihak perusahaan asuransi yang menyalahgunakan data pribadi nasabahnya.

PENUTUP

A. Kesimpulan

Berdasarkan hasil analisis dan pembahasan, maka dapat disimpulkan sebagai berikut:

1. Kebijakan dalam mengatasi kebocoran data nasabah asuransi jiwa pada era literasi digital memerlukan kerangka regulasi yang responsif dan implementatif dengan menitikberatkan pada penguatan tata kelola data serta penerapan standar keamanan informasi yang berlapis. Perusahaan asuransi dituntut untuk mengadopsi mekanisme perlindungan data berbasis teknologi mutakhir, seperti enkripsi, autentikasi multi-faktor dan sistem deteksi dini terhadap potensi pelanggaran. Selain itu, peran Otoritas Jasa Keuangan (OJK) sebagai pengawas memastikan kepatuhan terhadap regulasi perlindungan data pribadi, sehingga setiap pelanggaran dapat ditindak secara tegas dan memberikan efek jera.
2. Kebijakan perlindungan data nasabah asuransi jiwa di era literasi digital menuntut pendekatan yang komprehensif, adaptif dan berbasis pada prinsip kehati- hatian. Peningkatan pemanfaatan teknologi informasi harus diimbangi dengan penguatan regulasi, implementasi sistem keamanan siber yang memadai, serta pengawasan yang berkelanjutan. Selain itu, sinergi antara lembaga regulator, perusahaan asuransi dan pemangku kepentingan lainnya menjadi krusial dalam memastikan bahwa pengelolaan data pribadi nasabah dilakukan secara akuntabel dan sesuai dengan ketentuan hukum yang berlaku. Dengan demikian, risiko kebocoran data dapat diminimalisasi, sekaligus meningkatkan kepercayaan publik terhadap industri asuransi jiwa.

B. Saran

Berdasarkan kesimpulan di atas, maka disarankan beberapa hal sebagai berikut:

1. Pemerintah dan OJK sebagai pengawas diharapkan memperkuat kerangka regulasi terkait perlindungan data pribadi dengan merumuskan kebijakan yang lebih komprehensif, adaptif, dan berorientasi pada perkembangan teknologi digital. Perusahaan asuransi jiwa disarankan untuk meningkatkan kapasitas sistem keamanan informasi melalui penerapan teknologi mutakhir, seperti enkripsi end-to-end, sistem autentikasi berlapis, serta audit keamanan secara berkala. Penguatan tata kelola data juga perlu dilakukan dengan mengadopsi prinsip privacy by design dan privacy by default dalam setiap proses bisnis. Langkah ini penting untuk meminimalisasi potensi kebocoran data sekaligus memastikan bahwa pengelolaan informasi nasabah dilakukan secara transparan dan akuntabel.
2. Kebijakan perlindungan terhadap kebocoran data nasabah asuransi jiwa era literasi digital menuntut adanya pendekatan yang sistematis, terintegrasi dan berlandaskan pada prinsip perlindungan data pribadi. Penguatan regulasi yang adaptif terhadap perkembangan teknologi informasi disertai dengan implementasi standar keamanan siber yang komprehensif, menjadi elemen krusial dalam meminimalisasi risiko kebocoran data. Selain itu, optimalisasi fungsi pengawasan oleh otoritas terkait serta penerapan prinsip akuntabilitas oleh perusahaan asuransi

E-ISSN: 2828-3910

jiwa merupakan faktor penting dalam memastikan bahwa pengelolaan data nasabah dilakukan secara aman dan sesuai dengan ketentuan hukum yang berlaku.

E-ISSN: 2828-3910

Daftar Pustaka

Fauzi, W, 2019, Hukum Asuransi Di Indonesia, University Press, Andalas.

Fitriani, E & Nurhadi, W, 2021, Perlindungan Data Pribadi di Era Digital: Studi Kasus Indonesia, PT. Refika Utama, Bandung.

Hanifan, N, 2020, Perlindungan Data Pribadi Sebagai Bagian Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang Undangan Di Negara Lain, Citra Aditya Bakti, Bandung.

Jimly Asshiddiqie dan Hafid Abbas, 2010, Hak Asasi Manusia Dalam Konstitusi Indonesia Dari UUD 1945 Sampai dengan Perubahan UUD 1945 Tahun 2002,

Edisi Kelima, Prenada Media, Group, Jakarta.

Mulyati, 2017, Aspek Perlindungan Hukum Atas Data Pribadi Nasabah Pada Penyelenggaraan Layanan Internet Banking, Fakultas Syariah dan Hukum, UIN AR-RANIRY Darussalam, Aceh.

Nudirman Munir, 2017, Pengantar Hukum Siber Indonesia, Edisi Ketiga, Rajawali Perss, Jakarta.

Ramlan, 2023, Metode Penelitian Hukum Dalam Pembuatan Karya Ilmiah, Cetakan Pertama, UMSU PRESS, Medan.

Resa Raditio, 2014, Aspek Hukum Transaksi Elektronik, Graha Ilmu, Jakarta.

Sigid Suseno, 2012, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung.

Sudaryo, Y, 2020, Digital Marketing dan Fintech di Indonesia, Penerbit Andi, Jakarta.

Adi Rachmawan, Tantangan dan Solusi Terkait dengan Keamanan Data dan Privasi Pengguna, https://online.ciputra.ac.id/ke amanan-data/.

Chen, H & Zhao, Y, 2021, A Survey on Data Breach Detection and Prevention, Journal of Cyber Security Technology, 5(3), https://doi.org/10.1080/23742 917.2021.1945603.

Dwi Fajar, 2025, Literasi Digital Untuk Perlindungan Data Pribadi,https://mail.jurnalptik .id/index.php/JIK/article/view
/454/198, diaksespada 2 Oktober.

European Union Agency for Cybersecurity (ENISA), 2023, Data Breach: How to Handle It. Retrieved from https://www.enisa.europa.eu/t opics/csirt-cert-services/data-breach.

Lee, S. M & Lee, K. H, 2022,

Exploring The Impact Of Data Breaches On Firm Performance And Market Reactions, Journal of Business Ethics, 176(4), https://doi.org/10.1007/s1055 1-022-05142-0.

Mahuli, Jenda Ingan, 2023, Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital, All Fields of Science Journal Liaison Academia and Sosiety (3),(4).

Mohamad Soleh, 2024, Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital, Journal of Government, Social and Politics, Volume 11 Number 1, E-ISSN: 2721-9232.

Osmain Husain, 2025, Digital Privacy Definition: What Is Digital Privacy & Digital Safety, https://www.enzuzo.com/blo g/digital-privacy-definition, diakses pada 2 Oktober.

E-ISSN: 2828-3910

Payment Card Industry Data Security Standard (PCI DSS), 2022, PCI DSS Requirements and Security Assessment Procedures, Retrieved from https://www.pcisecuritystand ards.org/document_library.

Rosadi, S. D, 2018, Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia, Veritas, Vol 4(1).

Symantec, 2022, Internet Security Threat Report, Retrieved from https://www.broadcom.com/c ompany/newsroom/press- releases?filtr.

United States FederalTrade Commission (FTC), 2024, Protecting Personal Information: A Guide for Business, Retrieved from https://www.ftc.gov/tips advice/business center/privacy-and- security/protecting-personal- information.