KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.2, No.3 Mei 2025
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 474-485
DOI : https://doi.org/10.61722/jinu.v2i3.4525

STRATEGI MANAJEMEN DATA PRIVASI DALAM ERA DIGITAL PADA PERUSAHAAN DAN BISNIS MODERN

Zahfira Halim
zahfirahalim28@gmail.com
Universitas Islam Negeri Sumatera Utara
Muhammad Irwan Padli Nasution
irwannst@uinsu.ac.id.
Universitas Islam Negeri Sumatera Utara
Korespondensi penulis: *zahfirahalim28@gmail.com*

Abstract *The purpose of this study is to analyze the data privacy management strategies implemented by modern companies and businesses in addressing the challenges of the digital era. This research adopts a descriptive qualitative method using a library research approach, examining various academic sources, regulations, and corporate case studies. The findings reveal that effective data privacy management strategies include the implementation of clear internal policies, the use of security technologies such as encryption and multi-factor authentication, as well as regular audits and privacy education. Furthermore, transparency with consumers regarding the use of personal data plays a crucial role in building public trust. These findings highlight the importance of integrating policies, technology, and education as the main foundation for safeguarding data privacy in the digital age.*

Keywords: Data Privacy, Data Management, Digital Era, Information Security, Corporate Strategy and Bussines.

AbstrakTujuan dari penelitian ini adalah untuk menganalisis strategi manajemen data privasi yang diterapkan oleh perusahaan dan bisnis modern dalam menghadapi tantangan era digital. Penelitian ini menggunakan metode kualitatif deskriptif melalui pendekatan studi literatur (library research) yang mengkaji berbagai sumber akademik, regulasi, serta studi kasus perusahaan. Hasil kajian menunjukkan bahwa strategi manajemen data privasi yang efektif meliputi penerapan kebijakan internal yang jelas, pemanfaatan teknologi pengamanan seperti enkripsi dan otentikasi ganda, serta pelaksanaan audit dan edukasi privasi secara berkala. Selain itu, transparansi terhadap konsumen dalam hal penggunaan data pribadi juga menjadi faktor penting dalam membangun kepercayaan publik. Temuan ini menggarisbawahi pentingnya integrasi antara kebijakan, teknologi, dan edukasi sebagai fondasi utama dalam menjaga privasi data di era digital.

Kata Kunci: Privasi Data, Manajemen Data, Era Digital, Keamanan Informasi, Strategi Perusahaan dan Bisnis

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam cara perusahaan beroperasi dan berinteraksi dengan pelanggan. Di era digital ini, data pribadi telah menjadi aset yang sangat berharga bagi perusahaan. Data digunakan untuk memahami preferensi konsumen, meningkatkan pengalaman pengguna, serta mendukung pengambilan keputusan yang lebih tepat. Namun, dengan semakin banyaknya data yang dikumpulkan, diolah, dan disimpan, muncul pula tantangan besar terkait privasi dan keamanan data. Oleh karena itu, manajemen data privasi yang efektif sangat penting bagi perusahaan untuk menghindari risiko kebocoran data dan menjaga kepercayaan pelanggan.

Received Maret 28, 2025; Revised April 30, 2025; Mei 10, 2025
* Zahfira Halim, zahfirahalim28@gmail.com

Data telah menjadi sumber daya yang sangat berharga di dunia bisnis yang semakin bergantung pada teknologi digital (Groves : 2020). Perusahaan menggunakan data pribadi untuk menyusun strategi pemasaran, mempersonalisasi produk dan layanan, serta meningkatkan hubungan dengan pelanggan. Penggunaan data yang tepat dapat menghasilkan keuntungan kompetitif yang signifikan. Namun, pengelolaan data pribadi yang tidak sesuai dapat menimbulkan masalah serius, baik dari sisi hukum maupun reputasi perusahaan.

Meskipun manfaat pengelolaan data sangat besar, tantangan yang dihadapi perusahaan juga tidak kalah besar. Salah satu tantangan utama adalah melindungi data dari kebocoran atau pencurian yang dapat merusak kepercayaan konsumen (Kesan & Hayes : 2021). Selain itu, perusahaan juga harus memastikan bahwa data yang dikumpulkan digunakan dengan cara yang sah dan sesuai dengan keinginan konsumen. Kurangnya transparansi dalam pengumpulan dan penggunaan data sering kali menjadi salah satu faktor yang memicu ketidakpercayaan konsumen terhadap perusahaan.

Regulasi mengenai perlindungan data pribadi telah diterapkan secara ketat di banyak negara. Di Indonesia, UU Perlindungan Data Pribadi (UU PDP) yang baru saja disahkan menuntut perusahaan untuk lebih hati-hati dalam mengelola data pribadi (Pemerintah Republik Indonesia, 2022). Perusahaan diharuskan mendapatkan persetujuan eksplisit dari konsumen sebelum mengumpulkan data mereka dan memberikan hak kepada individu untuk mengakses, mengubah, dan menghapus data pribadi mereka. Regulasi internasional seperti GDPR juga menjadi pedoman bagi perusahaan yang beroperasi secara global.

Penggunaan teknologi yang tepat sangat penting dalam melindungi data pribadi. Teknologi enkripsi, autentikasi multi-faktor, dan firewall adalah beberapa contoh teknologi yang digunakan untuk melindungi data dari ancaman eksternal (Whittingham : 2022). Selain itu, sistem pemantauan yang terus-menerus dapat membantu mendeteksi dan merespons kebocoran data secara cepat. Implementasi teknologi ini juga membantu perusahaan dalam memastikan kepatuhan terhadap regulasi yang berlaku.

Transparansi dalam pengumpulan dan penggunaan data pribadi adalah kunci dalam menjaga kepercayaan konsumen (Smith & Whelan : 2021). Perusahaan harus memberikan informasi yang jelas mengenai bagaimana data pribadi mereka dikumpulkan, digunakan, dan disimpan. Dengan memberikan kontrol yang lebih besar kepada konsumen atas data mereka, perusahaan dapat memperkuat hubungan dengan pelanggan dan meningkatkan loyalitas. Hal ini juga akan mengurangi risiko pelanggaran privasi dan memberikan kepastian bagi konsumen bahwa data mereka dikelola dengan baik.

Berdasarkan temuan yang ada, perusahaan perlu mengadopsi beberapa langkah strategis untuk mengelola data pribadi secara efektif (IT Governance Institute : 2022). Pertama, perusahaan harus menyusun kebijakan privasi yang jelas dan mudah dipahami oleh konsumen. Kedua, penggunaan teknologi pengamanan yang canggih harus diutamakan untuk melindungi data dari ancaman eksternal. Ketiga, perusahaan harus

mengedukasi karyawan mengenai pentingnya privasi data dan memberikan pelatihan terkait kebijakan privasi. Keempat, audit rutin perlu dilakukan untuk memastikan bahwa perusahaan selalu mematuhi regulasi yang berlaku dan menjaga keamanan data.

KAJIAN TEORI

1. Konsep Data Privasi

Privasi data atau perlindungan data pribadi adalah hak individu untuk mengontrol pengumpulan, penggunaan, penyimpanan, dan distribusi informasi pribadi yang berkaitan dengan dirinya. Informasi pribadi ini mencakup data yang dapat mengidentifikasi seseorang, seperti nama, alamat, nomor identitas, data kesehatan, lokasi, dan informasi digital lainnya. (Muhammad Iqbal Iskandar :2024). Data privasi merujuk pada hak individu untuk mengontrol bagaimana data pribadi mereka dikumpulkan, digunakan, dan dibagikan. Oleh karena itu, perlindungan terhadap data pribadi sangat penting untuk menjaga privasi individu dan menghindari penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

Dalam penelitian (Matthew Kosinski dan Amber Forrest : 2023) Terdapat elemen Kunci dalam Konsep Privasi Data yaitu sebagai berikut :

1. **Kendali Individu** : Individu berhak menentukan siapa yang dapat mengakses dan menggunakan data mereka, menjaga otonomi dalam era digital.
2. **Data Pribadi** : Meliputi informasi yang mengidentifikasi seseorang, seperti nama, alamat, dan nomor identitas, yang dilindungi oleh UU PDP di Indonesia.
3. **Prinsip Perlindungan Data**: Mencakup keabsahan, transparansi, keamanan, minimisasi data, dan akuntabilitas dalam pengelolaan data pribadi.
4. **Privacy by Design** : Privasi dipertimbangkan sejak awal dalam desain sistem dan proses bisnis untuk mengurangi risiko pelanggaran data.
5. **Hak Privasi** : Individu memiliki hak untuk mengakses, mengubah, atau menghapus data pribadi mereka dan mengontrol penggunaannya.

2. Manajemen Data Privasi dalam Era Digital

Manajemen data dalam konteks digital mengacu pada proses pengumpulan, penyimpanan, pemrosesan, dan pengelolaan data untuk tujuan bisnis. (Privy : 2024) menyatakan bahwa dalam bisnis modern, data digunakan untuk meningkatkan efisiensi operasional, mempersonalisasi produk dan layanan, serta mendukung pengambilan keputusan yang lebih baik. Namun, manajemen data yang buruk dapat menyebabkan kerugian serius bagi perusahaan, baik dari segi reputasi maupun hukum.

Dalam penelitian (Kadek Rima Anggen Suari & I Made Sarjana : 2023) Strategi Perlindungan Data Pribadi terdiri dari beberapa poin yaitu :

1. **Peningkatan Keamanan Sistem**: Penerapan standar keamanan seperti enkripsi data, deteksi aktivitas anomali, dan sertifikasi sistem menjadi penting agar hanya pihak berwenang yang dapat mengakses informasi sensitif.

2. **Pendidikan dan Kesadaran Publik**: Edukasi kepada masyarakat mengenai pentingnya perlindungan data dapat meningkatkan kewaspadaan dan kemampuan individu dalam menjaga informasi pribadinya dari risiko digital.
3. **Kebijakan Privasi yang Transparan**: Perusahaan wajib menyediakan kebijakan privasi yang jelas, mencakup jenis data yang dikumpulkan, tujuan penggunaan, serta prosedur jika terjadi pelanggaran data.
4. **Penggunaan Alat Keamanan Pribadi**: Penggunaan antivirus, firewall, dan autentikasi dua faktor menjadi langkah penting bagi individu untuk mengamankan akses terhadap data pribadinya.
5. **Penguatan Regulasi**: Diperlukan regulasi yang tegas dan komprehensif seperti UU PDP, guna menegakkan hak privasi dan memberikan sanksi tegas bagi pelanggaran data.

3. **Regulasi Perlindungan Data**

Regulasi perlindungan data bertujuan untuk memberikan hak kepada individu terkait data pribadi mereka dan mengharuskan perusahaan untuk bertanggung jawab dalam pengelolaannya. Menurut (Domi Dwi Kurniasandi. et al : 2024), regulasi perlindungan data pribadi seperti UU Perlindungan Data Pribadi di Indonesia (UU PDP) memberikan pedoman yang jelas tentang bagaimana data pribadi harus dikelola dan melindungi konsumen dari potensi penyalahgunaan. Regulasi ini juga mendorong perusahaan untuk menjaga kepatuhan terhadap prinsip-prinsip perlindungan data.

Beberapa tujuan utama dari UU PDP meliputi:

1. **Melindungi hak privasi individu**: Mengatur pengumpulan, penggunaan, dan pengelolaan data pribadi untuk mencegah penyalahgunaan.
2. **Menjamin keamanan informasi**: Memastikan bahwa data pribadi dilindungi dengan baik dari kebocoran dan penyalahgunaan
3. **Mematuhi standar internasional**: Mengadaptasi regulasi dengan standar perlindungan data internasional seperti GDPR dari Uni Eropa

4. **Peran Teknologi dalam Perlindungan Data**

Teknologi memainkan peran penting dalam melindungi data pribadi dari ancaman eksternal. Ramadhan (2021) menjelaskan bahwa teknologi seperti enkripsi, autentikasi multi-faktor, dan sistem firewall dapat meningkatkan keamanan data pribadi yang disimpan oleh perusahaan. Penerapan teknologi ini memungkinkan perusahaan untuk melindungi data dari serangan cyber dan menjaga integritas informasi yang sangat penting bagi pelanggan.

(Sarjan Sakti : 20240 dalam penelitiannya : Peran Teknologi dalam Perlindungan Data Privasi terdapat beberapa poin yaitu :

1. **Blockchain**
   Memberikan transparansi dan akuntabilitas tinggi dalam pengelolaan data, mengurangi risiko penyalahgunaan informasi pribadi.

2. **Kecerdasan Buatan (AI)**
   Mendeteksi potensi pelanggaran data melalui analisis pola mencurigakan secara otomatis, memungkinkan pencegahan lebih dini.
3. **Enkripsi Data**
   Mengamankan data dengan mengubahnya ke dalam format terenkripsi, sehingga tidak dapat diakses tanpa izin.
4. **Autentikasi dan Kontrol Akses**
   Menggunakan metode seperti biometrik dan sistem berbasis peran untuk memastikan hanya pihak berwenang yang dapat mengakses data sensitif.
5. **Regulasi dan Standar Keamanan**
   UU PDP 2022 di Indonesia menjadi dasar hukum perlindungan data. Diperlukan standar keamanan tinggi seperti firewall dan sistem deteksi ancaman.
6. **Edukasi dan Kesadaran Publik**
   Masyarakat perlu diedukasi agar lebih peduli terhadap privasi data dan mampu menjaga informasi pribadinya secara mandiri.

5. **Transparansi dan Kepercayaan Konsumen**

Transparansi dalam pengumpulan dan penggunaan data pribadi merupakan faktor penting dalam menjaga hubungan yang baik antara perusahaan dan konsumen. Sari & Darmawan (2020) berpendapat bahwa perusahaan yang memberikan informasi yang jelas mengenai bagaimana data mereka dikumpulkan dan digunakan akan lebih dipercaya oleh konsumen. Kepercayaan ini dapat memperkuat loyalitas pelanggan dan mencegah potensi masalah hukum yang timbul akibat pelanggaran privasi.

Kepercayaan konsumen merupakan aset penting yang harus dijaga oleh setiap perusahaan. Pelanggaran data atau penyalahgunaan informasi dapat merusak reputasi perusahaan dan mengurangi kepercayaan konsumen. Oleh karena itu, perusahaan harus berkomitmen untuk menerapkan praktik etis dalam pengelolaan data, termasuk tidak menjual informasi pribadi tanpa izin (Pusko Media Indonesia : 2024)

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi pustaka (library research)**.** Tujuan dari pendekatan ini adalah untuk memperoleh pemahaman mendalam mengenai strategi manajemen data privasi dalam konteks perusahaan dan bisnis modern melalui penelaahan berbagai sumber literatur yang relevan.

Data yang digunakan dalam penelitian ini berasal dari berbagai referensi sekunder, seperti artikel ilmiah, jurnal nasional terakreditasi, buku akademik, laporan kebijakan pemerintah, serta regulasi terkait perlindungan data pribadi**,** khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**.** Penelusuran literatur dilakukan melalui database online seperti Garuda Ristekdikti, SINTA**,** Google Scholar, dan situs resmi instansi pemerintahan.

Analisis data dilakukan dengan cara mengelompokkan informasi berdasarkan tem**a**, seperti prinsip-prinsip perlindungan data, peran teknologi, strategi manajemen data di perusahaan, dan tantangan privasi di era digital. Selanjutnya, informasi yang diperoleh dianalisis secara kritis dan disajikan secara deskriptif untuk menggambarkan berbagai pendekatan dan strategi yang telah dan dapat diterapkan oleh organisasi atau perusahaan dalam mengelola data pribadi.

Keabsahan data dalam penelitian ini diperkuat dengan triangulasi sumber, yaitu membandingkan informasi dari beberapa referensi yang berbeda guna memastikan konsistensi dan keakuratan isi.

Melalui metode ini, diharapkan penelitian mampu memberikan kontribusi teoretis maupun praktis dalam memahami dan mengembangkan strategi manajemen data privasi yang efektif di era digital.

HASIL DAN PEMBAHASAN

Hasil

Dalam era digital yang semakin berkembang, perlindungan data pribadi menjadi isu yang sangat penting bagi perusahaan dan bisnis modern di Indonesia. Mengelola data pribadi dengan aman dan bertanggung jawab adalah kunci untuk menjaga kepercayaan pelanggan serta mematuhi regulasi yang berlaku. Berdasarkan studi literatur terhadap berbagai jurnal nasional, dokumen kebijakan, dan laporan penelitian terkini, terdapat beberapa strategi utama yang digunakan oleh organisasi untuk mengelola data pribadi secara efektif. Strategi-strategi ini dapat dibagi ke dalam tiga pilar utama: teknologi, kebijakan, dan kesadaran pengguna. Temuan ini menunjukkan bahwa implementasi yang efektif dari ketiga pilar tersebut sangat penting dalam menciptakan sistem manajemen data yang aman dan terlindungi.

1. Penggunaan Teknologi Keamanan Informasi

Perusahaan-perusahaan di Indonesia semakin menyadari pentingnya penggunaan teknologi dalam menjaga keamanan data pribadi. Salah satu teknologi yang paling umum diterapkan adalah enkripsi, yang berfungsi untuk mengamankan data selama proses pengiriman atau penyimpanan, sehingga data hanya dapat diakses oleh pihak yang berwenang. Selain itu, firewall digunakan untuk memantau dan mengontrol lalu lintas data antara jaringan internal dan eksternal guna mencegah potensi serangan atau akses tidak sah. Teknologi autentikasi ganda juga banyak diterapkan sebagai lapisan keamanan tambahan, yang mengharuskan pengguna untuk melakukan verifikasi identitas melalui dua metode berbeda sebelum dapat mengakses data sensitif.

Selain teknologi tersebut, perusahaan juga menggunakan sistem deteksi intrusi untuk memantau dan menganalisis pola aktivitas di dalam jaringan guna mengidentifikasi potensi ancaman secara real-time. Penggunaan teknologi ini membantu perusahaan dalam mengurangi risiko kebocoran data, sekaligus memastikan data pribadi pelanggan dan informasi sensitif lainnya tetap aman. Dengan mengintegrasikan berbagai teknologi keamanan informasi ini, perusahaan dapat memberikan perlindungan yang lebih kuat

terhadap data pribadi dan menghindari potensi pelanggaran yang dapat merugikan reputasi dan kepercayaan pelanggan.

2. Implementasi Kecerdasan Buatan (AI)

Kecerdasan buatan (AI) kini menjadi salah satu teknologi yang semakin banyak digunakan untuk mendeteksi dan mencegah kebocoran data pribadi di perusahaan-perusahaan Indonesia. AI dapat memantau dan menganalisis aktivitas pengguna dalam lingkungan digital untuk mendeteksi anomali atau pola perilaku yang tidak biasa, yang berpotensi mengindikasikan adanya kebocoran data atau serangan siber. Teknologi ini dapat mengidentifikasi aktivitas yang mencurigakan, seperti akses tidak sah terhadap data pribadi atau penyalahgunaan hak akses oleh pegawai internal, sehingga tindakan pencegahan dapat segera diambil. Di sektor fintech dan e-commerce, di mana transaksi digital sangat sering terjadi, penerapan AI membantu dalam mendeteksi potensi risiko lebih awal dan mengurangi kerugian akibat kebocoran data.

Di samping itu, AI juga digunakan untuk meningkatkan efisiensi dalam pengelolaan data pribadi, terutama dalam hal analisis dan pemrosesan data dalam jumlah besar. Dalam implementasinya, AI bekerja dengan menganalisis data transaksi pengguna secara otomatis, mengidentifikasi pola, dan memberikan rekomendasi terkait pengelolaan data yang lebih aman. AI juga dapat digunakan untuk menyaring data yang sensitif dan memastikan bahwa hanya data yang relevan dan dibutuhkan yang disimpan, sementara data yang tidak perlu dapat dihapus dengan aman. Dengan demikian, kecerdasan buatan dapat memperkuat upaya perlindungan data pribadi dan meningkatkan keandalan sistem keamanan di berbagai sektor.

3. Eksperimen dengan Teknologi Blockchain

Beberapa perusahaan rintisan di Indonesia mulai menerapkan teknologi blockchain untuk meningkatkan transparansi dan keamanan dalam pengelolaan data pribadi. Blockchain dikenal sebagai teknologi yang dapat menyimpan data dalam bentuk blok yang terhubung secara terdesentralisasi dan aman, membuatnya sulit untuk dimanipulasi atau diubah tanpa persetujuan dari semua pihak yang terlibat. Dengan menggunakan blockchain, perusahaan dapat memastikan bahwa setiap transaksi atau perubahan yang terjadi pada data pribadi tercatat secara transparan dan tidak dapat diubah, memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan sistem penyimpanan data tradisional. Teknologi ini menjadi pilihan yang menarik untuk melindungi data pribadi dalam berbagai sektor, termasuk finansial, kesehatan, dan e-commerce.

Selain itu, teknologi blockchain juga memungkinkan penggunaan smart contracts, yang secara otomatis mengeksekusi perjanjian atau transaksi berdasarkan ketentuan yang telah disepakati, tanpa memerlukan pihak ketiga. Dengan demikian, blockchain tidak hanya memberikan tingkat keamanan yang lebih tinggi, tetapi juga meningkatkan efisiensi operasional perusahaan. Walaupun implementasi blockchain di Indonesia masih dalam tahap pengembangan dan percobaan, sejumlah perusahaan mulai melihat potensi besar dalam menggunakan teknologi ini untuk mengamankan data pribadi. Ke depannya,

penggunaan blockchain dapat menjadi solusi yang lebih andal untuk mengelola dan melindungi data pribadi pelanggan secara efektif.

4. Penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP)

Sejak diberlakukannya Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, perusahaan-perusahaan di Indonesia semakin didorong untuk memperkuat kebijakan internal terkait pengelolaan data pribadi. UU PDP mewajibkan setiap organisasi untuk menetapkan petugas perlindungan data (Data Protection Officer/DPO) yang bertugas untuk mengawasi kepatuhan terhadap regulasi dan menjaga kerahasiaan data pribadi yang dikelola oleh perusahaan. Selain itu, perusahaan juga diwajibkan untuk menginformasikan kepada konsumen mengenai bagaimana data mereka akan digunakan, serta memperoleh persetujuan eksplisit dari pengguna sebelum mengumpulkan atau memproses data pribadi. Penerapan undang-undang ini memberikan dasar hukum yang kuat bagi perusahaan dalam melaksanakan kewajiban perlindungan data pribadi.

Lebih lanjut, UU PDP juga mewajibkan perusahaan untuk melaporkan insiden pelanggaran data dalam waktu tertentu kepada otoritas yang berwenang dan kepada individu yang terdampak. Hal ini bertujuan untuk memastikan bahwa setiap kebocoran atau pelanggaran data ditangani secara transparan dan tepat waktu, serta memberikan perlindungan yang lebih baik kepada konsumen. Dengan adanya regulasi yang jelas ini, perusahaan di Indonesia dapat lebih mudah mengimplementasikan kebijakan perlindungan data yang sesuai dengan standar internasional dan memperkuat kepercayaan publik terhadap kemampuan mereka dalam mengelola data pribadi dengan aman.

5. Peningkatan Edukasi dan Kesadaran Karyawan serta Konsumen

Meskipun teknologi dan kebijakan menjadi dua pilar utama dalam pengelolaan data pribadi, peningkatan kesadaran pengguna, baik di kalangan karyawan maupun konsumen, juga memainkan peran yang sangat penting. Banyak perusahaan di Indonesia mulai menyadari bahwa tanpa pemahaman yang kuat dari seluruh pihak terkait, kebijakan dan teknologi keamanan data tidak akan cukup efektif. Oleh karena itu, perusahaan mulai mengadakan pelatihan dan seminar internal untuk meningkatkan pemahaman karyawan tentang pentingnya perlindungan data pribadi dan cara mengidentifikasi potensi ancaman terhadap keamanan data. Pelatihan ini bertujuan untuk membangun budaya keamanan digital di tempat kerja, sehingga setiap individu tahu bagaimana cara menjaga data pribadi dengan aman dan mengurangi risiko kebocoran data.

Di sisi konsumen, beberapa perusahaan juga telah mengadakan kampanye edukasi untuk meningkatkan kesadaran masyarakat tentang pentingnya menjaga privasi data pribadi mereka. Hal ini mencakup memberikan informasi mengenai hak-hak konsumen terkait data pribadi, seperti hak untuk mengakses, mengubah, atau menghapus data pribadi yang telah diberikan kepada perusahaan. Peningkatan kesadaran ini diharapkan dapat menciptakan ekosistem digital yang lebih aman, di mana baik karyawan maupun konsumen memiliki pemahaman yang lebih baik tentang pentingnya menjaga kerahasiaan data pribadi dalam menghadapi risiko yang semakin kompleks

Tabel 1
Perbandingan Antara Perusahaan Yang Menggunakan Manajemen Privasi Data dan Yang Tidak Mengimplementasikannya Dalam Bisnis Modern:

Aspek	Menggunakan Manajemen Privasi Data	Tidak Menggunakan Manajemen Privasi Data
Keamanan Data	Data pribadi dilindungi dengan sistem keamanan canggih (enkripsi, firewall, AI) dan kepatuhan terhadap regulasi.	Data lebih rentan terhadap kebocoran dan serangan siber karena minimnya perlindungan.
Kepatuhan terhadap Regulasi	Mematuhi peraturan perlindungan data seperti UU PDP, dengan pengawasan dari petugas perlindungan data (DPO).	Tidak mematuhi regulasi yang berlaku, berisiko dikenakan sanksi atau denda.
Reputasi Perusahaan	Meningkatkan kepercayaan pelanggan dan reputasi perusahaan sebagai entitas yang menghargai privasi.	Reputasi perusahaan bisa rusak akibat kebocoran data atau penyalahgunaan informasi pelanggan.
Pengelolaan Risiko	Mampu mengidentifikasi dan mengurangi risiko kebocoran data secara efektif, menggunakan teknologi dan kebijakan pencegahan.	Risiko kebocoran data lebih tinggi, dan kerugian akibat insiden dapat sangat merugikan perusahaan.
Penggunaan Teknologi	Menggunakan teknologi seperti enkripsi, autentikasi ganda, AI, dan blockchain untuk meningkatkan perlindungan data.	Mengabaikan teknologi perlindungan data, meningkatkan potensi ancaman terhadap sistem.
Pendidikan dan Kesadaran	Mempunyai program pelatihan untuk karyawan dan edukasi kepada konsumen mengenai privasi data dan perlindungannya.	Tidak ada upaya untuk mendidik karyawan atau konsumen mengenai pentingnya privasi data.
Transparansi Data	Menyediakan transparansi penuh mengenai pengelolaan data pribadi, serta memberi kontrol kepada konsumen.	Data pribadi sering kali dikelola secara tidak transparan tanpa memberi kontrol kepada konsumen.
Tanggapan terhadap Insiden	Siap melaporkan insiden pelanggaran data secara cepat dan memberikan tindakan perbaikan sesuai regulasi.	Kurangnya respons yang cepat dan jelas terhadap kebocoran data atau

		pelanggaran, berpotensi memperburuk masalah.
Kepercayaan Pelanggan	Meningkatkan loyalitas dan kepuasan pelanggan karena perlindungan data yang lebih baik.	Kehilangan kepercayaan pelanggan, yang dapat menyebabkan penurunan pangsa pasar.
Inovasi dan Kompetitivitas	Dapat berinovasi dan berkembang dengan aman, menarik investor yang peduli terhadap perlindungan data.	Inovasi terbatas, dan potensi kerugian bisnis tinggi akibat kebocoran data yang dapat merusak peluang kompetitif.

Pembahasan

Temuan tersebut menunjukkan bahwa strategi manajemen data privasi dalam era digital pada perusahaan dan bisnis modern menuntut pendekatan yang menyeluruh dan berkelanjutan. Penerapan teknologi keamanan seperti enkripsi dan sistem deteksi intrusi (IDS) sangat krusial dalam menjaga kerahasiaan data. Strategi ini menjadi pondasi teknis utama dalam upaya pencegahan kebocoran data yang makin sering terjadi akibat serangan siber (Ramadhan, 2021).

Penerapan kecerdasan buatan juga menunjukkan peran penting dalam strategi ini. Melalui pembelajaran mesin, AI mampu melakukan pemantauan data secara real-time dan mengenali pola-pola yang tidak biasa—hal yang tidak selalu dapat ditangani oleh tenaga manusia. Ini memberikan keunggulan prediktif bagi perusahaan dalam mendeteksi risiko lebih awal (Kusumawati & Hidayat, 2023).

Selain teknologi, regulasi memiliki dampak yang signifikan. UU Perlindungan Data Pribadi mendorong terbangunnya struktur kebijakan internal yang memperjelas tanggung jawab dan alur pengelolaan data dalam perusahaan. Namun, implementasinya masih menghadapi kendala dalam hal kesiapan infrastruktur dan sumber daya manusia, terutama di kalangan usaha kecil menengah (Sari & Darmawan, 2020).

Strategi edukasi internal juga merupakan aspek penting. Kesadaran karyawan maupun konsumen tentang pentingnya menjaga informasi pribadi masih tergolong rendah. Hal ini mengindikasikan bahwa strategi perlindungan data harus dimulai dari perubahan budaya organisasi melalui edukasi berkelanjutan, bukan hanya dari aspek teknologi atau regulasi semata.

Secara keseluruhan, strategi manajemen data privasi di era digital menuntut integrasi antara **penguatan teknologi, penyusunan kebijakan yang jelas, dan pemberdayaan manusia** dalam menghadapi risiko privasi digital yang kian meningkat. Perusahaan yang mampu menggabungkan ketiga aspek ini akan lebih siap menghadapi tantangan privasi data sekaligus meningkatkan kepercayaan konsumen di era transformasi digital yang pesat.

Tabel 2. Strategi Manajemen Data Privasi di Era Digital

Strategi Utama	Penjelasan Singkat	Implementasi di Indonesia

Enkripsi dan Sistem Keamanan	Melindungi data melalui teknologi seperti firewall, VPN, dan autentikasi ganda	Digunakan luas oleh sektor perbankan dan fintech
Kecerdasan Buatan (AI)	Mendeteksi ancaman melalui analisis pola digital	Mulai diterapkan di sektor startup dan e-commerce
Blockchain	Menyimpan data secara transparan dan tidak dapat dimodifikasi	Digunakan terbatas di startup logistik dan data
Kepatuhan terhadap UU PDP	Regulasi nasional dalam pengelolaan data dan perlindungan hak individu	Berlaku wajib sejak 2022 untuk semua badan usaha
Edukasi Privasi Digital	Pelatihan dan kampanye untuk meningkatkan kesadaran privasi pengguna	Masih terbatas, perlu diperluas secara nasional

KESIMPULAN

Dalam menghadapi tantangan era digital, perusahaan dan bisnis modern di Indonesia harus menerapkan strategi yang komprehensif untuk menjaga privasi data pelanggan dan operasional mereka. Berdasarkan hasil studi, strategi utama yang dapat diterapkan mencakup penggunaan teknologi keamanan informasi seperti enkripsi dan autentikasi ganda, penerapan kecerdasan buatan (AI) untuk mendeteksi ancaman, serta eksperimen dengan blockchain untuk meningkatkan transparansi dan keamanan data. Selain itu, penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) juga menjadi langkah penting dalam memberikan landasan hukum yang jelas bagi pengelolaan data pribadi.

Pentingnya edukasi dan kesadaran pengguna juga menjadi faktor kunci dalam strategi perlindungan data, baik bagi karyawan perusahaan maupun konsumen. Meskipun masih terbatas, peningkatan pelatihan internal dan kampanye kesadaran dapat memperkuat budaya keamanan digital dalam perusahaan. Secara keseluruhan, perusahaan yang mampu mengintegrasikan teknologi, kebijakan, dan edukasi akan lebih siap dalam mengelola data pribadi dengan aman, membangun kepercayaan pelanggan, dan memenuhi regulasi yang berlaku di dunia digital yang semakin kompleks ini.

DAFTAR PUSTAKA

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum (JAH)*, 6(1), 132-146.

Dwi Kurniasandi, D., Aprilia, S. N., Indradjaja, N., & Chamdani. (2024). Regulasi Terkait Perlindungan Data Pribadi dalam Penggunaan Jasa E-Commerce. *Jurnal Ilmu Hukum Wijaya Putra*, 2(2), September.

European Commission. (2018). General Data Protection Regulation (GDPR). *Official Journal of the European Union*. Retrieved from https://gdpr.eu/

Groves, P. (2020). The Growing Importance of Data Privacy in the Digital Age. *Journal of Information Security*, 10(2), 23-34.

IT Governance Institute. (2022). Data Governance and Its Role in Protecting Privacy. Retrieved from https://itgid.org/insight/articles/data-governance-privacy.

Kesan, J. P., & Hayes, C. M. (2021). Privacy Law and Policy in the Digital Economy. *American Business Law Journal*, 58(1), 102-125.

Kosinski, M., & Forrest, A. (2023). IBM's Data Privacy.

Muhammad Iqbal Iskandar. (2024). Data Privacy: Prinsip Utama dalam Keamanan Informasi Pribadi. Retrieved from https://aplikas.com/blog/data-privacy/

Pemerintah Republik Indonesia. (2022). Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022. Retrieved from https://www.dpr.go.id/uu

Pusko Media Indonesia. (2024). Melindungi Data Pelanggan: Kebijakan Privasi yang Transparan pada Situs Web Anda. Retrieved from https://www.puskomedia.id/blog/melindungi-data-pelanggan-kebijakan-privasi-yang-transparan-pada-situs-web-anda/

Sarjan Sakti. (2024). Masa Depan Perlindungan Data Pribadi di Era Digital: Peluang dan Ancaman. Retrieved from https://kumparan.com/sarjan-lf/masa-depan-perlindungan-data-pribadi-di-era-digital-peluang-dan-ancaman-23vSurjCBF1

Smith, J., & Whelan, D. (2021). Data Protection and Security in the Age of Cloud Computing. *Journal of Cybersecurity Law*, 15(4), 56-71.

Whittingham, K. (2022). Ensuring Consumer Trust Through Data Privacy Transparency. *International Journal of Marketing*, 45(6), 98-110.