Grant Thornton

Mengamankan Data Pribadi dalam Proses Pembayaran Digital

December 2024

Mengamankan Data Pribadi dalam Proses Pembayaran Digital

Di tengah pesatnya perkembangan teknologi, pembayaran digital telah menjadi bagian dari kehidupan sehari-hari. Namun, di balik kemudahan tersebut, ancaman terhadap privasi dan keamanan data pribadi semakin meningkat. Industri perbankan dan jasa keuangan lainnya, termasuk jasa pembayaran *(payment services)*, seharusnya berada di garis depan dalam melindungi kerahasiaan data pribadi pengguna, nasabah, konsumen, karyawan, serta pihak ketiga lainnya. Oleh karena itu, penting bagi mereka untuk tidak hanya mematuhi regulasi yang berlaku, tetapi juga menjaga reputasi dan kepercayaan publik.

Mengacu pada Peraturan Bank Indonesia No. 22/23/ PBI/2020 tentang Sistem Pembayaran, terdapat dua jenis perusahaan yang diatur, yaitu Penyedia Jasa Pembayaran (PJP) dan Penyelenggara Infrastruktur Sistem Pembayaran (PIP). Penyedia Jasa Pembayaran (PJP) mencakup bank atau lembaga keuangan non-bank yang menyediakan layanan untuk memfasilitasi transaksi pembayaran. Sementara itu, Penyelenggara Infrastuktur Sistem Pembayaran (PIP) adalah pihak yang mengelola infrastruktur untuk memproses transaksi pembayaran.

Bagi organisasi secara umum, terutama PJP dan PIP, terdapat berbagai tantangan dalam melindungi data pribadi, mulai dari ancaman siber hingga tuntutan regulasi yang terus berkembang.

Jumlah serangan siber di Indonesia pada semester pertama tahun ini meningkat dibandingkan tahun sebelumnya,

6× Lipat

Sumber: *AwanPintar.id (2024)*

Evolusi Ancaman Siber

Ancaman siber berkembang sangat cepat, baik dari segi frekuensi maupun kompleksitas. Serangan seperti *phishing*, *malware*, *ransomware*, dan *DDoS* tidak hanya tetap mendominasi, tetapi juga semakin intensif. Permukaan serangan terus meluas, sementara modus operandinya semakin beragam. Menurut laporan analisis terbaru *AwanPintar.id* pada Agustus 2024, serangan siber di Indonesia meningkat enam kali lipat pada semester pertama tahun ini dibandingkan dengan periode yang sama pada tahun sebelumnya. Organisasi harus terus memperbaharui dan meningkatkan teknologi, proses, serta sumber daya keamanan untuk menghadapi ancaman ini, yang menjadi tantangan berkelanjutan.

Kepatuhan dengan Regulasi Tiap Negara

Regulasi pelindungan data pribadi berbeda di setiap negara. Perusahaan transnasional dan multinasional harus mematuhi berbagai hukum dan perundang-undangan yang berlaku di masing-masing yurisdiksi. Di Indonesia, Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 mengatur secara rinci tentang pengumpulan, pengolahan, penyimpanan, hingga penghapusan data pribadi. Kepatuhan terhadap regulasi ini membutuhkan pemahaman mendalam terhadap berbagai ketentuan yang berlaku, yang dapat menjadi tantangan tersendiri bagi organisasi.

Keterbatasan Sumber Daya dan Anggaran

Investasi dalam pelindungan data memerlukan sumber daya dan anggaran yang relatif signifikan. Tidak semua organisasi, terutama usaha skala kecil dan menengah (UKM), memiliki kecukupan sumber daya dan anggaran yang memadai untuk menjalankan proses, menyediakan teknologi dan layanan, merekrut personel yang kompeten, atau mengambil langkah-langkah lainnya. Menurut *Survei Keamanan Data 2023* yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), sekitar 60% UKM di Indonesia mengidentifikasi keterbatasan anggaran sebagai hambatan utama dalam mengadopsi teknologi keamanan canggih.

Kesalahan Manusia

Human error tetap menjadi salah satu penyebab utama kebocoran data, meskipun teknologi keamanan dan pelindungan data terus berkembang. Karyawan dan pengguna akhir sering kali menjadi titik terlemah dalam menghadapi berbagai insiden dan serangan. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 menekankan pentingnya pelatihan rutin bagi karyawan untuk menjaga keamanan data. Namun, penyelenggaraan pelatihan yang efektif dan efisien masih menjadi tantangan bagi banyak organisasi.

60%

UKM di Indonesia menganggap keterbatasan anggaran sebagai hambatan utama dalam mengadopsi teknologi keamanan canggih.

Sumber: *Survei Keamanan Data (20203)* oleh Asosiasi Penyelenggara Jasa Internwti Indonesia

Mengelola Data Pihak Ketiga

Organisasi sering berbagi data dengan pihak ketiga, seperti pemasok, mitra bisnis, perusahaan induk, perusahaan anak, pihak afiliasi, sampai dengan regulator. Meskipun data ini berada di luar kendali langsung organisasi, tanggung jawab untuk melindunginya tetap berada di tangan organisasi tersebut.

UU PDP mengatur bahwa organisasi harus memastikan pihak ketiga memiliki standar keamanan dan pelindungan data yang setidaknya setara dengan standar organisasi. Mengelola dan memastikan kepatuhan pihak ketiga ini merupakan tantangan tersendiri, terutama jika mereka tersebar di berbagai lokasi, lintas negara ataupun lintas benua.

Untuk mengatasi berbagai tantangan di atas, organisasi jasa pembayaran dapat mengambil beberapa langkah penting, antara lain:

1. **Memahami dan Mematuhi Peraturan Pelindungan Data**
   Kepatuhan terhadap UU No. 27 Tahun 2022 merupakan kewajiban yang tidak dapat diabaikan. Di dalamnya, termasuk pelaksanaan Penilaian Dampak Pelindungan Data *(Data Protection Impact Assessment)* dan pengangkatan Pejabat Pelindungan Data *(Data Protection Officer)*. Langkah ini tidak hanya bertujuan untuk memenuhi kewajiban hukum tetapi juga menjaga kepercayaan dan membangun landasan hubungan yang kuat dengan pengguna layanan.

2. **Menyusun Kebijakan dan Prosedur Pelindungan Data yang Kokoh**
   Organisasi harus memiliki kebijakan dan prosedur keamanan dan pelindungan data (pribadi) yang komprehensif, diterapkan secara konsisten, serta berkesinambungan. Kebijakan untuk bertujuan untuk mencegah terjadinya kebocoran maupun penyalahgunaan data pribadi. Seluruh karyawan perlu mengetahui, memahami, dan mematuhi kebijakan serta prosedur ini. Dengan demikian,mereka dapat secara kolektif berkontribusi dalam upaya pelindungan data yang efektif.

3. **Mematuhi Ketentuan Penyimpanan dan Retensi Data**
   Organisasi wajib mematuhi Pedoman Retensi Data sesuai dengan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Berdasarkan peraturan tersebut, data pribadi yang tersimpan di sistem elektronik harus disimpan setidaknya selama 5 (lima) tahun, kecuali ditentukan lain oleh peraturan perundang-undangan. Idealnya, organisasi juga memiliki kebijakan dan prosedur yang jelas terkait penyimpanan data pribadi dalam bentuk non-elektronik.

4. **Manfaatkan Teknologi Keamanan dan Pelindungan Data**
   Penerapan teknologi *(technical control)* seperti enkripsi, *masking*, *hashing*, otentikasi multi faktor, dan tokenisasi menjadi langkah penting untuk melindungi data dan informasi sensitif, termasuk data pribadi.
   Enkripsi dan masking digunakan untuk menjaga kerahasiaan data, hashing untuk menjaga integritas data, sementara otentikasi multi- faktor dan tokenisasi dapat dimanfaatkan untuk indentifikasi, verifikasi dan pemberian akses kepada pengguna. Selain itu, pemanfaatan alat *Data Loss Prevention* untuk memitigasi risiko kebocoran data, khususnya di aplikasi *instant messaging* sangat layak dipertimbangkan.

5. **Berhubungan dengan Pihak Ketiga Secara Bijak**
   Sebelum memutuskan untuk bekerja sama dengan pihak ketiga, penting untuk memilih mitra yang memiliki standar keamanan dan pelindungan data yang solid. Kontrak atau perjanjian dengan pihak ketiga harus mencantumkan klausul yang jelas mengenai tanggung jawab mereka dalam melindungi data pribadi.

6. **Melakukan Pengawasan dan Pengendalian Berkala**
   Pemeriksaan terhadap keamanan dan pelindungan data harus dilakukan secara rutin dan berkelanjutan untuk memastikan efektivitas kebijakan dan prosedur serta sudah kesesuaian dengan peraturan yang berlaku. Pemantauan terhadap akses, proses, dan aktivitas data pribadi memungkinkan organisasi untuk mendeteksi serta merespons ancaman dan insiden dengan cepat dan tepat.

7. **Memberikan Edukasi kepada Karyawan dan Pengguna Secara Rutin**
   Edukasi kepada karyawan dan pengguna mengenai data pribadi dan pelindungan data dilakukan secara rutin dan berkelanjutan. Desain, pelaksanaan, dan pengawasan program sosialisasi, penyuluhan, serta pelatihan dapat melibatkan divisi Sumber Daya Manusia (SDM), dengan dasar metriks yang relevan, jelas dan memadai.

Dengan langkah-langkah ini, perusahaan jasa pembayaran tidak hanya melindungi data pribadi pelanggan mereka, tetapi juga menunjukkan komitmen mereka terhadap keamanan dan privasi data di era digital untuk meningkatkan kepercayaan publik, membangun reputasi yang lebih baik, meningkatkan transparansi dalam pengelolaan data pribadi, serta mengurangi risiko pelanggaran data dan denda terkait.

Referensi

1. Laporan Hasil Analisis Terbaru AwanPintar Agustus 2024
   https://kumparan.com/kumparantech/serangan-siber-ke-ri-naik-6-kali-lipat-pada-h1-2024-mayoritas-dari-dalam-negeri-23PnYQpafrf
2. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
3. Pedoman Retensi Arsip Urusan Badan Usaha Bidang Perbankan (Peraturan Arsip Nasional No. 27 Tahun 2016).
4. Survei Keamanan Data 2024 oleh Asosiasi Penyelenggara Jasa Internet Indonesia
   https://survei.apjii.or.id/survei/group/9
5. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Grant Thornton

grantthornton.co.id