Grant Thornton

Membangun Kesadaran dan Kepatuhan Karyawan terhadap Pelindungan Data Pribadi

December 2024

Membangun Kesadaran dan Kepatuhan Karyawan terhadap Pelindungan Data Pribadi

Di era digital, perlindungan privasi data dan data pribadi telah menjadi perhatian utama di berbagai negara di dunia, termasuk Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menekankan pentingnya transparansi, akuntabilitas, serta kepatuhan terhadap prinsip-prinsip perlindungan data dalam aktivitas operasional organisasi. Salah satu kunci keberhasilan implementasi perlindungan data pribadi adalah kesadaran dan kepatuhan karyawan terhadap kebijakan dan regulasi yang berlaku [1][2].

Pemahaman karyawan mengenai pentingnya privasi data, data pribadi, dan UU PDP tidak cukup hanya bersifat teoritis; mereka juga perlu mampu menerapkannya dalam aktivitas sehari-hari di tempat kerja. Oleh karena itu, program pelatihan yang dirancang untuk membangun dan meningkatkan kesadaran tentang perlindungan data pribadi menjadi sangat penting. Pelatihan semacam ini bertujuan memastikan bahwa seluruh jajaran organisasi, mulai dari level operasional hingga manajemen, dapat memahami dan mematuhi kebijakan, prosedur, serta peraturan yang berlaku.

Pentingnya Kesadaran Pelindungan Data Pribadi

Seiring dengan meningkatnya frekuensi dan jumlah kebocoran data dan informasi pribadi yang dilaporkan di berbagai sektor industri, kebijakan dan prosedur organisasi terkait pelindungan data semakin diperketat dari waktu ke waktu. Menurut berbagai penelitian global[3][4], lebih dari separuh kasus kebocoran data disebabkan oleh kesalahan manusia, yang sebagian besar berakar pada kurangnya pemahaman mengenai pengelolaan data dan informasi (pribadi) yang benar.

Di sisi lain, kepatuhan terhadap regulasi bukan hanya soal menghindari sanksi, tetapi juga membangun kepercayaan publik, termasuk di kalangan konsumen dan mitra bisnis. Dengan meningkatkan kesadaran karyawan tentang pelindungan data pribadi, perusahaan tidak hanya memenuhi kewajiban regulasi, tetapi juga memperkuat reputasi bisnis dan meningkatkan loyalitas pelanggan.

Program Pelatihan Pelindungan Data Pribadi

Agar organisasi dapat memastikan bahwa karyawan memahami dan mematuhi UU PDP, diperlukan pendekatan yang sistematis dan berkelanjutan melalui program pelatihan. Beberapa jenis pelatihan yang dapat diimplementasikan oleh perusahaan, antara lain:

1. Pelatihan Dasar Pelindungan Data Pribadi

Pelatihan dasar bertujuan untuk memberikan pemahaman umum kepada karyawan tentang konsep utama pelindungan data pribadi, termasuk definisi data pribadi, hak subjek data, serta prinsip-prinsip pemrosesan data yang aman. Pelatihan ini juga sebaiknya mencakup contoh nyata terkait dengan pelanggaran data yang pernah terjadi di industri tertentu untuk memberikan gambaran yang lebih konkret mengenai risiko yang dihadapi.

Pelatihan dasar ini idealnya diberikan kepada seluruh karyawan, baik pada saat *onboarding* maupun sebagai bagian dari pelatihan berkelanjutan. Dengan memastikan bahwa setiap karyawan memahami dasar-dasar pelindungan data pribadi, perusahaan dapat membangun fondasi kepatuhan yang kokoh.

2. Pelatihan Teknis untuk Tim IT dan Keamanan Informasi

Tim IT dan keamanan informasi memegang peran krusial dalam menjaga keamanan data perusahaan. Oleh karena itu, mereka memerlukan pelatihan yang lebih mendalam dan teknis. Pelatihan ini sebaiknya mencakup aspek-aspek seperti enkripsi data, pengelolaan akses, pengaturan *firewall*, serta prosedur penanganan insiden jika terjadi kebocoran data.

Selain itu, mereka juga perlu dilatih mengenai implementasi kebijakan keamanan yang sesuai dengan standar internasional seperti ISO/IEC 27001, yang mengatur tentang sistem manajemen keamanan informasi. Pelatihan yang berfokus pada praktik terbaik dalam mitigasi risiko juga sangat penting untuk memastikan data pribadi tetap terlindungi, bahkan saat serangan siber.

3. Pelatihan Khusus untuk Pemrosesan Data Sensitif

Bagi karyawan yang secara langsung menangani data sensitif, seperti data medis, keuangan, atau informasi rahasia perusahaan, pelatihan khusus harus disediakan. Program pelatihan ini harus lebih fokus pada pengelolaan data tersebut dengan aman, pemahaman mengenai persyaratan hukum khusus, serta teknik mitigasi risiko yang relevan.

Contoh pelatihan yang direkomendasikan termasuk pelatihan cara mengamankan akses ke data sensitif, proses pseudonimisasi dan anonimitasi data, serta prosedur khusus jika data sensitif harus dipindahkan atau diakses oleh pihak ketiga.

4. Simulasi Kebocoran Data

Simulasi adalah metode yang efektif untuk menguji kesiapan karyawan dan sistem keamanan organisasi dalam menghadapi insiden kebocoran data. Dalam simulasi ini, karyawan dilibatkan dalam skenario pelanggaran data yang dirancang menyerupai kejadian nyata, sehingga mereka dapat mempraktikkan langkah-langkah yang harus diambil dalam menghadapi situasi tersebut.

Simulasi kebocoran data juga membantu organisasi mengidentifikasi berbagai celah dalam sistem keamanan dan memperbaikinya sebelum terjadi pelanggaran yang sebenarnya.

5. Pelatihan Eksternal dan Sertifikasi

Untuk mendukung program pelatihan, organisasi dapat mempertimbangkan untuk mengirimkan karyawan ke pelatihan eksternal guna memperoleh sertifikasi tertentu yang diselenggarakan oleh asosiasi profesi bidang privasi dan/atau keamanan siber.

Beberapa sertifikasi internasional yang dapat dipertimbangkan, antara lain:

- *Certified Information Privacy Professional (CIPP)*,
- *Certified Information Privacy Manager (CIPM)*,
- *Certified Information Privacy Technologist (CIPT)*,
- *Certified Information Systems Security Professional (CISSP)*,
- dan *Certified Information Security Manager (CISM)*.

Sertifikasi ini dapat meningkatkan kompetensi karyawan dalam hal data pribadi, privasi data, pelindungan data, keamanan informasi, serta keamanan siber.

Menilai Efektivitas Program Pelatihan

Mengadakan pelatihan saja tidak cukup untuk memastikan bahwa karyawan memahami dan menerapkan prinsip-prinsip pelindungan data pribadi. Oleh karena itu, organisasi perlu menilai efektivitas program pelatihan secara berkala dan berkelanjutan.

Beberapa cara yang dapat digunakan untuk mengevaluasi efektivitas pelatihan, antara lain:

Penilaian Pra dan Pasca Pelatihan

Sebelum dan sesudah pelatihan, organisasi dapat melakukan penilaian melalui kuis atau tes singkat untuk mengukur pemahaman karyawan terhadap materi yang telah disampaikan. Hasil tes ini dapat digunakan untuk menilai apakah pelatihan tersebut perlu disesuaikan.

Pengawasan dan Pemeriksaan Internal

Melalui pengawasan dan pemeriksaan internal, organisasi dapat menilai sejauh mana pelatihan yang telah diberikan berdampak pada sikap, perilaku, dan kepatuhan karyawan terhadap pelindungan data pribadi, baik secara langsung maupun tidak langsung.

Pengujian Keamanan Berkala

Pengujian keamanan berkala, seperti *vulnerability assessment* dan *penetration testing*, dapat membantu organisasi untuk menilai penerapan pengetahuan dan keterampilan yang diperoleh karyawan dari pelatihan teknis maupun non-teknis. Hasil pengujian ini dapat menjadi dasar untuk menyusun pelatihan lanjutan yang lebih spesifik.

Umpan Balik

Survei kepada karyawan mengenai pengalaman mereka selama mengikuti pelatihan dapat memberikan wawasan tambahan mengenai area mana yang perlu disesuaikan, diperbaiki, atau dikembangkan. Umpan balik dari karyawan juga menjadi sumber informasi berharga dalam merancang pelatihan yang lebih relevan dan menarik.

Penutup

Membangun kesadaran dan kepatuhan terhadap pelindungan data pribadi memerlukan daya upaya yang sistematis, terstruktur dan berkelanjutan. Melalui program pelatihan yang tepat dan evaluasi berkala, hasil kolaborasi dan koordinasi antara berbagai pemangku kepentingan — termasuk unit operasional, teknologi informasi (TI), teknologi, risiko, kepatuhan, keamanan, sumber daya manusia, dan tata kelola— organisasi dapat memastikan bahwa karyawan tidak hanya memahami peraturan yang berlaku, tetapi juga memiliki pengetahuan dan keterampilan yang memadai untuk menerapkan pelindungan data pribadi secara efisien dan efektif dalam kegiatan sehari-hari mereka.

Written by:
Matthew Jason Johanes
IT Advisory

Referensi

1. CISOMag (2020). "Psychology of Human Error" Could Help Businesses Prevent Security Breaches. [daring]. Tersedia di https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches [Diakses 2 Oktober 2024].
2. Financier Worldwide (Maret 2024). A comparative analysis of employee data protection: US vs. EU. [daring]. Tersedia di https://www.financierworldwide.com/a-comparative-analysis-of-employee-data-protection-us-vs-eu [Diakses 1 Oktober 2024].
3. Mandatly (2024). The Role of Employee Training in GDPR Compliance and Data Security. [daring]. Tersedia di https://mandatly.com/gdpr-compliance/the-role-of-employee-training-in-gdpr-compliance-and-data-security [Diakses 1 Oktober 2024].
4. Privacy International (2023). Global Data Breach Research 2023. [daring]. Tersedia di https://privacyinternational.org/ [Diakses 5 Oktober 2024].
5. Republik Indonesia (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. [daring]. Tersedia di https://peraturan.go.id/id/uu-no-27-tahun-2022 [Diakses 3 Oktober 2024].
6. Verizon Business (2023). DBIR Report 2023. [daring]. Tersedia di https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ [Diakses 2 Oktober 2024].

Grant Thornton

grantthornton.co.id