



Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

GDPR

Sekilas

Anda mungkin pernah mendengar undang-undang (UU) GDPR atau General Data Protection Regulation. UU ini dibuat oleh Uni Eropa dan efektif berlaku 25 Mei 2018. Menjangkau semua organisasi yang menangani informasi individu setiap penduduk Uni Eropa (European Union/EU), dimanapun organisasi tersebut berada. GDPR mewajibkan organisasi menjaga privasi dan keamanan informasi pribadi setiap penduduk UE. Untuk menjamin kepatuhan pada GDPR, beberapa prinsip utama perlu dimengerti dan dijalankan.

Setiap orang berhak atas privasi. Organisasi perlu menjaga privasi itu dengan cara membatasi data pribadi yang bisa diperoleh, diproses dan juga memberikan perlindungan pada data tersebut. Hak privasi ini mencakup semua informasi baik secara mandiri atau digunakan berbarengan dengan informasi lainnya, yang bisa digunakan untuk mengidentifikasi seseorang penghuni UE. Bisa ini berupa alamat, nomer pasport, nomer SIM, rincian financial, biometrik, keanggotaan UE, sejarah kesehatan, data lokasi atau informasi yang berhubungan dengan seksualitas individu, kepercayaan atau orientasi politik. UU ini berlaku bagi 'manusia alami', artinya pribadi seseorang yang hidup. Berikut in beberapa prinsip GDPR yang harus dipatuhi:



Data pribadi seseorang harus diproses berdasar hukum, secara adil dan transparan.



Orang harus mendapatkan penjelasan data apa yang dikumpulkan dan kegunaannya.



Data personal harus diperoleh untuk tujuan tertentu, jelas dan sah. Tidak boleh digunakan untuk tujuan lain yang berbenturan dengan hal diatas.



Data pribadi hanya boleh disimpan dan diolah sesuai kebutuhan dan dalam jangka waktu tertentu saja.



Data pribadi harus dalam kondisi terkini dan akurat.



Orang berhak mendapatkan salinan data mereka dan meminta data tersebut tidak digunakan lagi atau dalam kasus tertentu, dihapus seluruhnya.



Organisasi harus menerapkan cara pengamanan tertentu untuk melindungi data pribadi terhadap musibah atau kejadian perusakan, penghilangan, perubahan atau pembocoran.



Selain itu, organisasi perlu memastikan semua staff yang menangani data pribadi mendapatkan cukup pelatihan perihal pengaman dan perlindungan data.

Tindakan proteksi yang dilakukan untuk melindungi data pribadi harus menjamin tingkat keamanan yang sebanding dengan sensitifitas data. Bila faktor resiko pada data membesar, upaya dan biaya tindakan perlindungan juga harus disesuaikan. Beragam tindakan itu harus dikaji dan disempurnakan seperlunya. Pencatatan yang rapi perihal privasi, kebijakan dan tindakan dibutuhkan untuk menunjukkan kepatuhan. Selain itu, organisasi secara legal terikat untuk menjalankan tindakan, seperti pengkajian kontrak dan kerja-sama, untuk melindungi data pribadi pada saat dipindahkan ke pihak ketiga khususnya pihak ketiga diluar UE. Terakhir, bila terjadi peretasan data pribadi, organisasi harus melaporkan kejadian tersebut maksimal 72 jam setelah penemuan peristiwa itu. Ketidak patuhan oraganisasi dalam mematuhi GDPR bisa terancam denda hingga 4% dari pendapatan global, menjadikan GDPR salah satu UU beresiko termahal di dunia.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: <http://www.bipimax.net>

Editor Tamu

Brian Honan adalah CEO BH Consulting, perusahaan konsultan keamanan siber dan pengamanan data berbasis di Dublin Irlandia. Brian adalah penasehat khusus Europol Cybercrime Center (EC3), pendiri CERT pertama di Irlandia, dan sebagai anggota badan penasehat beberapa perusahaan keamanan inovatif. Brian ada di www.linkedin.com/in/brianhonan atau Twitter [@brianhonan](https://twitter.com/brianhonan).



Daftar Pustaka

GDPR Overview For Individuals and Organizations: <http://gdprandyou.ie>

The GDPR Regulation: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679>

OUCH! Terjemahan dan Berkas: <https://www.sans.org/u/D88>

OUCH! diterbitkan oleh SANS "Security Awareness" dan didistribusikan sesuai lisensi Creative Commons BY-NC-ND 4.0. Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan perubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi www.sans.org/security-awareness/ouch-newsletter. Dewan Redaksi: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Diterjemahkan oleh: T. Gunawan