Refleksi · 16 Mei 2026

← Sebelumnya·Berikutnya →

Rahasia profesi di era digital

Ketika komunikasi antara profesional dan kliennya dilakukan melalui saluran yang secara teknis tidak memadai, rahasia tersebut tidak rusak pada hari kebocoran. Rahasia itu sudah rusak jauh sebelumnya, pada saat pemilihan alat.

Masalah yang hampir tidak dilihat oleh siapa pun

Seorang pengacara menerima dokumen rahasia dari klien di teleponnya. Seorang dokter mendiskusikan diagnosis yang rumit dengan rekannya. Seorang psikolog mengoordinasikan perawatan pasien dengan psikiater. Seorang konsultan pajak mengirimkan data SPT yang menunggu peninjauan. Semua melakukannya melalui pesan instan. Dan hampir tidak ada yang berhenti sejenak untuk memikirkan di mana pesan-pesan itu sebenarnya berakhir.

Jawabannya dalam banyak kasus sama saja: di server yang tidak dikontrol oleh profesional tersebut, di negara yang undang-undangnya belum tentu dia ketahui, dikelola oleh perusahaan yang model bisnisnya adalah – dalam istilah ekonomi langsung – akumulasi data. Pesan tersebut mungkin dienkripsi saat transit. Namun begitu sampai di server, itu adalah salinan yang disimpan dalam infrastruktur pihak ketiga, tunduk pada keputusan operasional, hukum, dan komersial dari pihak ketiga tersebut. Bukan keputusan profesional.

Apa yang dikatakan undang-undang

Peraturan Umum Perlindungan Data Eropa sangat tegas dalam Pasal 32: siapa pun yang memproses data pribadi harus menerapkan tindakan teknis dan organisasional yang "tepat" untuk menjamin tingkat keamanan yang sesuai dengan risiko. Ketepatan tindakan tidak diukur dengan "apa yang diklaim aplikasi lakukan", melainkan dengan risiko nyata. Jika data klien berakhir di server yang yurisdiksinya tidak menjamin tingkat perlindungan yang setara dengan Wilayah Ekonomi Eropa, pengontrol data – yaitu profesional tersebut – menanggung risiko yang mungkin tidak dia sadari sepenuhnya.

Dan ini bukan hanya tentang GDPR. Rahasia profesi, yang diatur secara khusus untuk pengacara, dokter, psikolog, auditor, jurnalis, dan lainnya, mengharuskan komunikasi dengan klien bersifat rahasia. Bukan "serahasia mungkin". Rahasia tanpa syarat. Jika saluran teknis yang digunakan tidak dapat menjamin hal ini, profesional tersebut menanggung risiko yang tidak diizinkan oleh etika profesinya.

Paradoksnya adalah risikonya tidak terlihat. Tidak ada yang mengaudit perpesanan kantor. Tidak ada yang meminta kontrak pemrosesan data dari penyedia obrolan. Risiko baru muncul ketika sudah terlambat: kebocoran, pelanggaran yang dipublikasikan, perintah pengadilan yang dieksekusi di benua lain tanpa pemberitahuan kepada pengguna.

Apa yang dibutuhkan seorang profesional secara teknis

Apa yang dibutuhkan oleh seseorang dengan kewajiban rahasia profesi sebenarnya sangat sederhana dari sudut pandang persyaratan:

- Saluran di mana pesan langsung dikirim dari perangkat pengirim ke perangkat penerima, tanpa melewati server perantara yang menyimpan salinan.
- Infrastruktur yang yurisdiksi dan kebijakannya selaras dengan GDPR melalui konstruksi, bukan melalui pernyataan.
- Cara untuk mengidentifikasi diri dengan lawan bicara tanpa perlu menyerahkan kontak profesional (nama klien, nomor telepon, buku kontak) kepada pihak ketiga.
- Sistem yang dapat diverifikasi – tidak berdasarkan kata-kata penyedia – untuk mengonfirmasi bahwa pesan sampai ke orang yang tepat.

Ini bukanlah daftar yang menuntut. Ini sebenarnya adalah apa yang dianggap wajar dalam komunikasi profesional pra-digital. Surat tercatat memenuhi semua kriteria ini. Panggilan telepon dari sentral kantor ke sentral klien juga demikian. Yang aneh bukanlah jaminan ini diminta hari ini: yang aneh adalah jaminan tersebut telah hilang dalam transisi ke saluran digital, tanpa ada yang menyadarinya.

Perbedaan antara mengenkripsi dan tidak menyimpan

Ada metafora yang berguna. Mengenkripsi pesan dan menyimpannya di server setara dengan menaruh dokumen di dalam brankas dan meninggalkan brankas itu di rumah orang asing. Brankasnya bagus. Dokumen tersebut pada prinsipnya tidak dapat dibaca. Namun dokumen itu *masih berada di rumah orang lain*. Dan orang itu bisa saja menerima perintah pengadilan, mengalami serangan siber, mengubah ketentuan layanannya, dibeli oleh perusahaan lain dengan etika yang berbeda, atau bisa menghilang besok.

Alternatif strukturalnya – bukan prosedural, bukan berdasarkan kepercayaan – adalah dokumen tersebut tidak pernah keluar dari kantor. Dokumen tersebut berpindah langsung dari meja profesional ke meja klien tanpa ada perantara apa pun. Inilah yang dilakukan komunikasi point-to-point antar perangkat secara teknis: ia menghilangkan perantara. Bukannya perantara itu jahat. Hanya saja dalam kasus rahasia profesi, perantara itu *tidak diperlukan*. Dan apa yang tidak diperlukan, dalam sistem apa pun yang ingin aman, harus dihilangkan sebagai prinsip.

Pertanyaan tentang tanggung jawab

Pada akhirnya, pertanyaan yang harus dijawab oleh setiap profesional dengan kewajiban rahasia dengan jawaban 'ya' yang tegas adalah sebagai berikut:

> Jika besok percakapan dengan salah satu klien saya bocor dan pengadilan atau asosiasi profesi bertanya kepada saya bagaimana saya mengelola kerahasiaan, dapatkah saya secara teknis membuktikan bahwa saluran yang saya gunakan tidak menyimpan salinan di infrastruktur pihak ketiga? Dapatkah saya membuktikan bahwa data tersebut tidak pernah keluar dari perangkat dua orang yang terlibat dalam percakapan? Dapatkah saya, tanpa bergantung pada kata-kata perusahaan dari benua lain, membuktikan bahwa kerahasiaan dijamin oleh arsitektur dan bukan oleh janji?

Jika jawabannya tidak, masalahnya bukan pada alat itu secara konkret. Masalahnya adalah sebuah tanggung jawab telah didelegasikan kepada sebuah alat yang alat tersebut tidak dirancang untuk menopangnya. Itu seperti menaruh berkas rahasia di dalam amplop transparan dan percaya bahwa tukang pos tidak akan melihat ke dalamnya.

Alat yang dipilih seorang profesional untuk berkomunikasi dengan kliennya mengatakan banyak hal tentang bagaimana dia menghargai kepercayaan mereka. Ada alat yang dirancang agar kepercayaan itu tidak bergantung pada janji, melainkan pada arsitektur. Dan ada alat yang tidak demikian. Mengetahui perbedaannya adalah bagian dari pekerjaan.

Kerangka normatif yang dikutip

- Peraturan (Uni Eropa) 2016/679 (GDPR), khususnya Pasal 5, 25 (perlindungan data melalui desain) dan 32 (keamanan pemrosesan).
- Peraturan perundang-undangan di Indonesia mengenai rahasia profesi (misalnya UU Advokat, UU Praktik Kedokteran, Kode Etik Psikologi).
- Kitab Undang-Undang Hukum Pidana (KUHP) tentang pembocoran rahasia.
- Kode etik asosiasi profesi mengenai kerahasiaan dan rahasia jabatan.

← SebelumnyaEnkripsi tidak berarti privasi: apa yang dikatakan metadata tentang AndaBerikutnya →GDPR dan pesan profesional: mengapa sebagian besar melanggar aturan tanpa menyadarinya

Bacaan terbaru

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bawa artikel ini bersama Anda ke mana pun Anda membutuhkannya.

↓ Markdown ↓ Teks murni ↓ PDF

File akan diunduh ke perangkat Anda. Dari sana Anda dapat menyimpannya, mengimpornya ke Solo2, atau membagikannya di mana pun Anda mau. Cuadernos tidak memutuskan tujuan untuk Anda.

Segel lilin · SHA-256 19d320f11a917cc36f3c089ec800b07a643adb38772ccc9c52d4706e7fa751f0

Cuadernos Lacre · Publikasi dari Menzuri Gestión S.L. ·
ditulis oleh R.Eugenio · disunting oleh tim Solo2.