Analisis · 16 Mei 2026

← Sebelumnya·Berikutnya →

GDPR dan pesan profesional: mengapa sebagian besar melanggar aturan tanpa menyadarinya

Hampir setiap kantor, klinik, atau perusahaan konsultan mengirimkan dokumen klien melalui aplikasi yang servernya berlokasi di luar Wilayah Ekonomi Eropa. Tanpa niat buruk, tetapi dalam banyak kasus melanggar peraturan tanpa ada yang memperingatkan mereka.

Dokumen yang melakukan perjalanan lebih jauh dari yang Anda kira

Situasi sehari-hari: seorang konsultan pajak menerima dokumen berisi data klien melalui perpesanan. Seorang staf penjualan meneruskan penawaran kepada rekannya melalui obrolan. Seorang dokter berbagi laporan klinis dengan mitra kerjanya melalui jalur yang sama. Tidak ada yang berpikir dua kali. Itu normal. Itu nyaman. Itulah yang dilakukan setiap hari di setiap kantor di setiap kota di Eropa.

Namun dokumen ini, dalam banyak kasus, baru saja melakukan perjalanan ke server di Amerika Serikat. Dokumen itu disimpan – meskipun hanya sementara, meskipun "dienkripsi saat diam" – di cloud yang tidak dikontrol oleh profesional tersebut maupun kliennya. Dokumen itu telah melewati sistem yang secara teknis dapat mengindeks metadata yang terkait dengan konten. Dan Peraturan Umum Perlindungan Data Eropa memiliki sesuatu yang cukup jelas untuk dikatakan tentang hal ini.

Apa yang dituntut oleh norma

GDPR – dan sebagai perluasannya yurisprudensi Pengadilan Kehakiman Uni Eropa (terutama keputusan Schrems II, C-311/18, tahun 2020) – menetapkan bahwa data pribadi warga negara Eropa harus dilindungi secara memadai. Jika data ini meninggalkan Wilayah Ekonomi Eropa, pengontrol data harus menjamin bahwa penerima menawarkan tingkat perlindungan yang "secara substansial setara" dengan tingkat perlindungan Eropa. Dalam praktiknya, ini berarti bahwa pengiriman data klien melalui layanan yang servernya berada di bawah yurisdiksi AS, tanpa melakukan penilaian dampak dan tanpa menerapkan jaminan pelengkap – klausul kontrak standar, tindakan teknis tambahan seperti enkripsi yang dapat diverifikasi, dll. – dapat merupakan pelanggaran peraturan. Meskipun sampai saat ini belum ada yang mengatakan apa pun.

Dan ini bukan hanya tentang isi pesan. Metadata – siapa mengirim apa kepada siapa, kapan, seberapa sering, dari mana – juga merupakan data pribadi menurut peraturan, menurut interpretasi berulang dari Dewan Perlindungan Data Eropa. Layanan yang mengumpulkan metadata dari komunikasi profesional pengguna memproses data pribadi klien pengguna tersebut, tanpa sepengetahuan mereka atau memberikan persetujuan apa pun untuk pemrosesan tersebut.

Pola pikir umum – "saya hanya menggunakan aplikasi untuk menulis; aplikasi tersebut bukan penyedia data klien saya" – secara hukum salah. Jika data klien melewati infrastruktur pihak ketiga, pihak ketiga tersebut memproses data tersebut. Dan jika mereka memprosesnya, harus ada dasar hukum, kontrak pemrosesan data, dan jaminan yang memadai.

Siapa yang bertanggung jawab

Pertanyaan tentang siapa yang memikul tanggung jawab hukum bukanlah pertanyaan akademis. GDPR membedakan antara *pengontrol data* (siapa yang memutuskan data apa yang diproses dan untuk tujuan apa) and *prosesor* (siapa yang melakukannya secara material atas nama pengontrol). Profesional yang mengirimkan dokumen klien adalah pengontrol. Penyedia aplikasi pesan dalam banyak kasus adalah prosesor de facto. Tanpa kontrak pemrosesan – dan tanpa sebagian besar klausul yang seharusnya disertakan dalam kontrak semacam itu – pengontrol belum memenuhi kewajibannya.

Interpretasi lunaknya adalah: "sebagian besar profesional tidak mengetahui hal ini". Interpretasi kerasnya adalah: "ketidaktahuan akan hukum bukan merupakan alasan pemaaf". Dan interpretasi dari pengacara spesialis perlindungan data mana pun yang dikonsultasikan mengenai hal ini biasanya adalah interpretasi yang keras.

Untuk siapa hal ini penting secara konkret

Bagi setiap profesional atau perusahaan yang meskipun hanya sesekali beroperasi dengan informasi pribadi pihak ketiga:

- Pengacara yang menerima dokumentasi klien (kontrak, tuntutan, pernyataan, laporan aset).
- Dokter dan profesional kesehatan lainnya yang berbagi data kesehatan – yang dianggap berdasarkan Pasal 9 GDPR sebagai *kategori khusus* dengan rezim perlindungan yang diperkuat –.
- Konsultan pajak dan manajer administratif yang mengoperasikan data identifikasi, pajak, dan perbankan.
- Departemen sumber daya manusia yang mengelola dokumentasi kerja dan pribadi karyawan.
- Perwakilan komersial yang menerima detail kontak dan sering kali informasi bisnis yang sensitif dari prospek dan klien.

Dalam semua kasus, informasi dilindungi oleh GDPR. Dalam semua kasus, dalam praktik yang umum, informasi ini mengalir melalui saluran yang yurisdiksinya tidak memungkinkan mereka dinyatakan "secara substansial setara" dengan kerangka kerja Eropa tanpa jaminan tambahan. Bukan karena niat buruk. Karena kebiasaan. Dan karena infrastruktur teknologi yang selama lima belas tahun telah mengutamakan kenyamanan daripada kepatuhan.

Argumen "semua orang melakukannya"

Adalah bijaksana untuk mengantisipasi keberatan yang paling umum: "jika semua orang melakukannya, itu tidak mungkin menjadi masalah nyata". Ini adalah argumen yang sepenuhnya dapat dimengerti dan secara hukum tidak memiliki kekuatan apa pun. Fakta bahwa suatu praktik tersebar luas tidak menjadikannya sesuai dengan peraturan. Otoritas perlindungan data telah menjatuhkan sanksi dalam beberapa tahun terakhir kepada beberapa perusahaan tepatnya karena cara penggunaan perpesanan yang tampak tidak berbahaya hingga saat inspeksi.

Realitas operasional saat ini adalah bahwa risiko dalam hal probabilitas rendah – sangat jarang inspeksi dari Otoritas mengaudit alat perpesanan khusus dari kantor berukuran sedang – tetapi tinggi dalam hal dampak jika itu terwujud. Ini adalah risiko yang diambil sebagian besar orang tanpa mengetahui bahwa mereka mengambilnya. Artinya, tanpa mengevaluasi apakah alat yang digunakan sejalan dengan tanggung jawab hukum pengontrol data.

Jejak digital bersifat retroaktif

Ada argumen kedua, hampir simetris dengan yang sebelumnya, yang layak untuk diantisipasi: *"jika ini adalah masalah serius, administrasi pasti sudah mulai memantaunya"*. Realitas yang diamati saat ini memberikan pembenaran yang dangkal. Inspeksi karena penggunaan perpesanan yang tidak tepat di perusahaan kecil dan terutama pada wiraswasta hampir tidak ada saat ini – bukan karena perilaku tersebut diperbolehkan, melainkan

karena administrasi di sebagian besar UE kekurangan sumber daya manusia yang diperlukan untuk mengaudit jutaan entitas yang diwajibkan.

Inilah yang disiratkan oleh praktik yang diamati hari ini. Namun bukan itu yang disiratkan oleh dekade berikutnya. Dua vektor bertemu untuk mengubah keseimbangan dalam jangka waktu yang relatif singkat.

Pertama: jejak digital bersifat retroaktif. Setiap pesan yang dikirim melalui aplikasi dengan server pusat tetap terdaftar – setidaknya dalam metadata – dalam infrastruktur yang bertahan lama. Apa yang dikirim enam bulan lalu secara teknis masih dapat diaudit hari ini. Apa yang dikirim hari ini akan dapat diaudit dalam lima tahun ke depan. Tidak adanya inspeksi saat ini bukanlah jaminan tidak adanya inspeksi di masa depan. Ini adalah penundaan penilaian, bukan pembebasan.

Kedua: kapasitas inspeksi administratif akan tumbuh secara akselerasi. Pengenalan alat kecerdasan buatan dalam proses pemantauan menghilangkan hambatan manusia yang selama ini melindungi – secara de facto, bukan de jure – perusahaan kecil dan wiraswasta. Sistem yang mampu melakukan cross-reference metadata masif, pengembalian pajak, daftar komersial, dan kewajiban pemberitahuan pelanggaran keamanan tidak memerlukan inspektur: ia membutuhkan akses. Dan akses melalui permintaan kepada penyedia dengan kehadiran hukum di UE dalam kerangka normatif saat ini sepenuhnya dapat dilakukan.

Ditambah lagi faktor yang kurang teknis tetapi sama menentukannya: negara-negara Eropa berada dalam proses penambahan utang yang terus-menerus dan mereka perlu, hampir tanpa kecuali, memperluas basis pajak mereka. Sanksi administratif yang timbul dari ketidakpatuhan terhadap GDPR, dalam istilah fiskal murni, merupakan sumber pendapatan yang berkembang dan nyaman secara politik. Ini bukan dugaan: ini adalah tren yang dapat diamati dalam laporan tahunan otoritas perlindungan data Eropa, di mana total volume sanksi meningkat selama beberapa tahun fiskal berturut-turut.

Kesimpulan operasional bagi pengontrol data bukanlah alarmis melainkan tenang: **keputusan tentang bagaimana mengelola komunikasi dengan klien saat ini dievaluasi terhadap kapasitas inspeksi tahun di mana inspeksi dilakukan, bukan terhadap kapasitas saat ini.** Dan kapasitas itu dalam jangka waktu yang wajar akan sangat berbeda dari saat ini. Siapa pun yang mulai melakukan hal-hal dengan benar hari ini tidak hanya akan baik-baik saja mulai hari ini: jejak yang dihasilkan mulai saat ini akan sesuai dengan norma, dan ini secara retroaktif melindungi periode yang akan datang. Siapa pun yang melanjutkan seperti sebelumnya akan mengumpulkan jejak yang dapat diaudit yang kepatuhannya akan dievaluasi sesuai dengan standar – dan sumber daya – tahun-tahun mendatang.

Apa yang berubah dengan arsitektur yang berbeda

Terdapat alternatif teknis di mana data tidak disimpan dalam infrastruktur pihak ketiga, melainkan berpindah langsung dari perangkat pengirim ke perangkat penerima. Dalam arsitektur ini, kepatuhan terhadap GDPR terkait transfer internasional tidak bergantung pada klausul kontrak standar, atau pada niat baik penyedia, atau pada audit di masa depan. Ini bergantung pada fakta bahwa *tidak ada transfer*. Dan apa yang tidak ada tidak dapat dilanggar.

Ini bukan satu-satunya solusi dan bukan satu-satunya solusi yang mungkin. Namun ini berbeda secara struktural, dan kepatuhan normatif berhenti menjadi lampiran prosedural dan menjadi konsekuensi langsung dari desain. Bagi seorang profesional yang menjalankan tanggung jawabnya sebagai pengontrol data dengan serius, perbedaan itu sangat berarti.

Edisi Cuadernos berikutnya akan menganalisis secara rinci keputusan Schrems II dan implikasi praktisnya bagi perusahaan kecil dan menengah yang bergantung pada layanan cloud AS, lima tahun setelah publikasinya.

Sumber dan kerangka normatif

- Peraturan (Uni Eropa) 2016/679 (GDPR), khususnya Bab V tentang transfer internasional.
- CJUE C-311/18 ("Schrems II"), 16 Juli 2020.
- EDPB – Rekomendasi 01/2020 tentang tindakan yang melengkapi alat transfer.
- Otoritas Perlindungan Data – Laporan tahunan dengan kasuistik sanksi karena penggunaan pesan instan yang tidak tepat di lingkungan profesional.

← SebelumnyaRahasia profesi di era digitalBerikutnya →Ketika tidak ada siapa-siapa di tengah

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 60a3b66c01d3f7ee934b5db0151e0ae0c8d0b84bf6879aa4432c23a92c5ba5f7

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