Analisis · 16 Mei 2026

← Sebelumnya·Seterusnya →

GDPR dan pemesejan profesional: mengapa kebanyakan melanggar peraturan tanpa menyedarinya

Hampir setiap pejabat, klinik, atau firma perunding menghantar dokumen pelanggan melalui aplikasi yang pelayannya terletak di luar Kawasan Ekonomi Eropah. Tanpa niat jahat, tetapi dalam banyak kes melanggar peraturan tanpa ada yang memberi amaran kepada mereka.

Dokumen yang melakukan perjalanan lebih jauh daripada yang anda fikirkan

Situasi harian: seorang perunding cukai menerima dokumen yang mengandungi data pelanggan melalui pemesejan. Seorang ejen jualan meneruskan tawaran kepada rakannya melalui sembang. Seorang doktor berkongsi laporan klinikal dengan rakan sekerjanya melalui laluan yang sama. Tiada siapa yang berfikir dua kali. Ia normal. Ia mudah. Itulah yang dilakukan setiap hari di setiap pejabat di setiap bandar di Eropah.

Walau bagaimanapun dokumen ini, dalam banyak kes, baru sahaja melakukan perjalanan ke pelayan di Amerika Syarikat. Ia disimpan – walaupun hanya sementara, walaupun "disulitkan semasa diam" – di awan yang tidak dikawal oleh profesional tersebut mahupun pelanggannya. Ia telah melalui sistem yang secara teknikal dapat mengindeks metadata yang dikaitkan dengan kandungan. Dan Peraturan Umum Perlindungan Data Eropah mempunyai sesuatu yang cukup jelas untuk dikatakan tentang perkara ini.

Apa yang dituntut oleh norma

GDPR – dan sebagai peluasannya yurisprudensi Mahkamah Keadilan Kesatuan Eropah (terutamanya keputusan Schrems II, C-311/18, pada tahun 2020) – menetapkan bahawa data peribadi warganegara Eropah mesti dilindungi secara mencukupi. Jika data ini meninggalkan Kawasan Ekonomi Eropah, pengawal data mesti menjamin bahawa penerima menawarkan tahap perlindungan yang "secara substansial setara" dengan tahap perlindungan Eropah. Dalam praktiknya, ini bermakna bahawa penghantaran data pelanggan melalui perkhidmatan yang pelayannya berada di bawah bidang kuasa AS, tanpa melakukan penilaian impak dan tanpa melaksanakan jaminan pelengkap – klausa kontrak standard, tindakan teknikal tambahan seperti penyulitan yang dapat disahkan, dll. – boleh merupakan pelanggaran peraturan. Walaupun sehingga kini belum ada yang mengatakan apa-apa.

Dan ini bukan sahaja tentang kandungan mesej. Metadata – siapa menghantar apa kepada siapa, bila, seberapa kerap, dari mana – juga merupakan data peribadi menurut peraturan, menurut tafsiran berulang dari Lembaga Perlindungan Data Eropah. Perkhidmatan yang mengumpul metadata daripada komunikasi profesional pengguna memproses data peribadi pelanggan pengguna tersebut, tanpa pengetahuan mereka atau memberi sebarang persetujuan untuk pemprosesan tersebut.

Pola fikir biasa – "saya hanya menggunakan aplikasi untuk menulis; aplikasi tersebut bukan penyedia data pelanggan saya" – secara hukum adalah salah. Jika data pelanggan melalui infrastruktur pihak ketiga, pihak ketiga tersebut memproses data tersebut. Dan jika mereka memprosesnya, mesti ada dasar hukum, kontrak pemprosesan data, dan jaminan yang mencukupi.

Siapa yang bertanggungjawab

Persoalan tentang siapa yang memikul tanggungjawab undang-undang bukanlah soalan akademik. GDPR membezakan antara *pengawal data* (siapa yang memutuskan data apa yang diproses dan untuk tujuan apa) and *pemproses* (siapa yang melakukannya secara material bagi pihak pengawal). Profesional yang menghantar dokumen pelanggan adalah pengawal. Penyedia aplikasi mesej dalam banyak kes adalah pemproses de facto. Tanpa kontrak pemprosesan – dan tanpa sebahagian besar klausa yang sepatutnya disertakan dalam kontrak sedemikian – pengawal belum memenuhi kewajipannya.

Tafsiran lembutnya ialah: "kebanyakan profesional tidak mengetahui perkara ini". Tafsiran kerasnya ialah: "kejahilan tentang undang-undang bukanlah alasan pemaaf". Dan tafsiran daripada mana-mana peguam pakar perlindungan data yang dirujuk mengenai perkara ini biasanya ialah tafsiran yang keras.

Untuk siapa perkara ini penting secara konkrit

Bagi setiap profesional atau syarikat yang walaupun hanya sesekali beroperasi dengan maklumat peribadi pihak ketiga:

- Peguam yang menerima dokumentasi pelanggan (kontrak, tuntutan, kenyataan, laporan aset).
- Doktor dan profesional kesihatan lain yang berkongsi data kesihatan – yang dianggap berdasarkan Pasal 9 GDPR sebagai *kategori khas* dengan rejim perlindungan yang diperkukuh –.
- Perunding cukai dan pengurus pentadbiran yang mengendalikan data pengenalan, cukai, dan perbankan.
- Jabatan sumber manusia yang menguruskan dokumentasi kerja dan peribadi pekerja.
- Wakil komersial yang menerima butiran hubungan dan selalunya maklumat perniagaan yang sensitif daripada prospek dan pelanggan.

Dalam semua kes, maklumat dilindungi oleh GDPR. Dalam semua kes, dalam amalan yang biasa, maklumat ini mengalir melalui saluran yang bidang kuasanya tidak membolehkan mereka dinyatakan "secara substansial setara" dengan rangka kerja Eropah tanpa jaminan tambahan. Bukan kerana niat jahat. Kerana tabiat. Dan kerana infrastruktur teknologi yang selama lima belas tahun telah mengutamakan kemudahan daripada pematuhan.

Argumen "semua orang melakukannya"

Adalah bijaksana untuk menjangka bantahan yang paling biasa: "jika semua orang melakukannya, ia tidak mungkin menjadi masalah sebenar". Ini adalah argumen yang sepenuhnya boleh difahami dan dari segi undang-undang tidak mempunyai sebarang kekuatan. Fakta bahawa suatu amalan tersebar luas tidak menjadikannya mengikut peraturan. Pihak berkuasa perlindungan data telah menjatuhkan sanksi dalam beberapa tahun kebelakangan ini kepada beberapa syarikat tepat kerana cara penggunaan pemesejan yang kelihatan tidak berbahaya sehingga saat pemeriksaan.

Realiti operasi semasa ialah risiko dalam hal kebarangkalian adalah rendah – sangat jarang pemeriksaan dari Pihak Berkuasa mengaudit alat pemesejan khusus dari pejabat bersaiz sederhana – tetapi tinggi dalam hal impak jika ia berlaku. Ini adalah risiko yang diambil oleh kebanyakan orang tanpa mengetahui bahawa mereka mengambilnya. Bermakna, tanpa menilai sama ada alat yang digunakan sehaluan dengan tanggungjawab undang-undang pengawal data.

Jejak digital bersifat retroaktif

Ada argumen kedua, hampir simetri dengan yang sebelumnya, yang layak untuk dijangka: *"jika ini adalah masalah serius, pentadbiran pasti sudah mula memantaunya"*. Realiti yang diperhatikan pada masa ini memberikan kewajaran yang cetek. Pemeriksaan kerana penggunaan pemesejan yang tidak betul di syarikat kecil dan terutamanya pada bekerja sendiri hampir tidak wujud pada masa ini – bukan kerana tingkah laku tersebut dibenarkan, sebaliknya kerana pentadbiran di sebahagian besar EU kekurangan sumber manusia yang diperlukan untuk mengaudit berjuta-juta entiti yang diwajibkan.

Inilah yang disiratkan oleh amalan yang diperhatikan hari ini. Namun bukan itu yang disiratkan oleh dekad seterusnya. Dua vektor bertemu untuk mengubah keseimbangan dalam jangka masa yang relatif singkat.

Pertama: jejak digital bersifat retroaktif. Setiap mesej yang dihantar melalui aplikasi dengan pelayan pusat tetap berdaftar – sekurang-kurangnya dalam metadata – dalam infrastruktur yang bertahan lama. Apa yang dihantar enam bulan lalu secara teknikal masih boleh diaudit hari ini. Apa yang dihantar hari ini akan dapat diaudit dalam lima tahun akan datang. Ketiadaan pemeriksaan pada masa ini bukanlah jaminan ketiadaan pemeriksaan pada masa hadapan. Ini adalah penangguhan penilaian, bukan pembebasan.

Kedua: kapasiti pemeriksaan pentadbiran akan tumbuh secara akselerasi. Pengenalan alat kecerdasan buatan dalam proses pemantauan menghapuskan halangan manusia yang selama ini melindungi – secara de facto, bukan de jure – syarikat kecil dan bekerja sendiri. Sistem yang mampu melakukan cross-reference metadata masif, pulangan cukai, daftar komersial, dan kewajipan pemberitahuan pelanggaran keselamatan tidak memerlukan inspektor: ia memerlukan akses. Dan akses melalui permintaan kepada penyedia dengan kehadiran undang-undang di EU dalam rangka kerja normatif semasa sepenuhnya boleh dilakukan.

Ditambah lagi faktor yang kurang teknikal tetapi sama menentukannya: negara-negara Eropah berada dalam proses penambahan hutang yang berterusan dan mereka perlu, hampir tanpa kecuali, meluaskan asas cukai mereka. Sanksi pentadbiran yang timbul daripada ketidakpatuhan terhadap GDPR adalah dalam istilah fiskal murni, sumber pendapatan yang berkembang dan selesa secara politik. Ini bukan duga: ini adalah trend yang dapat diperhatikan dalam laporan tahunan pihak berkuasa perlindungan data Eropah, di mana jumlah volum sanksi meningkat selama beberapa tahun fiskal berturut-turut.

Kesimpulan operasi bagi pengawal data bukanlah alarmis melainkan tenang: **keputusan tentang bagaimana menguruskan komunikasi dengan pelanggan pada hari ini dinilai terhadap kapasiti pemeriksaan tahun di mana pemeriksaan dilakukan, bukan terhadap kapasiti semasa.** Dan kapasiti itu dalam jangka masa yang munasabah akan sangat berbeza daripada hari ini. Sesiapa yang mula melakukan perkara dengan betul hari ini tidak hanya akan baik-baik saja mulai hari ini: jejak yang dihasilkan mulai saat ini akan mengikut norma, dan ini secara retroaktif melindungi tempoh yang akan datang. Sesiapa yang meneruskan seperti sebelum ini akan mengumpul jejak yang boleh diaudit yang kepatuhannya akan dinilai mengikut standard – dan sumber daya – tahun-tahun mendatang.

Apa yang berubah dengan seni bina yang berbeza

Terdapat alternatif teknikal di mana data tidak disimpan dalam infrastruktur pihak ketiga, sebaliknya berpindah terus dari peranti pengirim ke peranti penerima. Dalam seni bina ini, pematuhan terhadap GDPR berkaitan pemindahan antarabangsa tidak bergantung pada klausa kontrak standard, atau pada niat baik penyedia, atau pada audit di masa hadapan. Ia bergantung pada fakta bahawa *tiada pemindahan*. Dan apa yang tidak wujud tidak boleh dilanggar.

Ini bukan satu-satunya penyelesaian dan bukan satu-satunya penyelesaian yang mungkin. Namun ia berbeza secara struktural, dan pematuhan normatif berhenti menjadi lampiran prosedur dan menjadi konsekuensi langsung daripada reka bentuk. Bagi seorang profesional yang menjalankan tanggungjawabnya sebagai pengawal data dengan serius, perbezaan itu sangat bermakna.

Edisi Cuadernos seterusnya akan menganalisis secara terperinci keputusan Schrems II dan implikasi praktikalnya bagi syarikat kecil dan sederhana yang bergantung pada perkhidmatan awan AS, lima tahun selepas penerbitannya.

Sumber dan rangka kerja normatif

- Peraturan (Kesatuan Eropah) 2016/679 (GDPR), khususnya Bab V tentang pemindahan antarabangsa.
- CJUE C-311/18 ("Schrems II"), 16 Julai 2020.
- EDPB – Syor 01/2020 tentang tindakan yang melengkapkan alat pemindahan.
- Pihak Berkuasa Perlindungan Data – Laporan tahunan dengan kasuistik sanksi kerana penggunaan mesej segera yang tidak tepat di persekitaran profesional.

← SebelumnyaRahsia profesional dalam era digitalSeterusnya →Apabila tiada sesiapa di tengah

Bacaan terkini

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bawa artikel ini bersama anda ke mana sahaja anda memerlukannya.

↓ Markdown ↓ Teks biasa ↓ PDF

Fail akan dimuat turun ke peranti anda. Dari sana anda boleh menyimpannya, mengimportnya ke Solo2, atau berkongsinya di mana sahaja anda mahu. Cuadernos tidak memutuskan destinasi untuk anda.

Mohor lilin · SHA-256 75a016c91560e3eff01d7586756437e40c5b4fdc6524e2905ba55460a046ea4b

Cuadernos Lacre · Penerbitan daripada Menzuri Gestión S.L. ·
ditulis oleh R.Eugenio · disunting oleh pasukan Solo2.