Reflexe · 16. května 2026

← Předchozí·Další →

Profesní tajemství v digitální éře

Pokud komunikace mezi profesionálem a jeho klientem probíhá technicky nevhodným kanálem, tajemství se neporuší v den úniku. Bylo porušeno mnohem dříve, v okamžiku výběru nástroje.

Abychom si rozuměli: Právník pošle smlouvu klienta přes WhatsApp. Lékař komentuje diagnózu přes Telegram. Nikomu to nepřipadá divné. Ale profesní tajemství se neporuší v den, kdy něco unikne — bylo porušeno ve chvíli, kdy byl zvolen komunikační kanál.

Problém, který téměř nikdo nevidí

Advokát obdrží na svůj telefon citlivý dokument od klienta. Lékař konzultuje s kolegou choulostivou diagnózu. Psycholog koordinuje s psychiatrem léčbu pacienta. Daňový poradce zasílá údaje z přiznání čekajícího na revizi. Všichni tak činí prostřednictvím instant messagingu. A téměř nikdo se nezastaví, aby se zamyslel nad tím, kde tyto zprávy skutečně končí.

Odpověď je ve většině případů stejná: na serveru, který profesionál nekontroluje, v zemi, jejíž legislativu nemusí nutně znát, spravovaném společností, jejímž obchodním modelem je – vyjádřeno přímými ekonomickými termíny – hromadění dat. Zpráva může být při přenosu šifrovaná. Jakmile však dorazí na server, je to kopie uložená v infrastruktuře třetí strany, která podléhá operativním, právním a komerčním rozhodnutím této třetí strany. Nikoli profesionála.

Co říká legislativa

Evropské obecné nařízení o ochraně osobních údajů je ve svém článku 32 jednoznačné: kdokoli zpracovává osobní údaje, musí uplatnit "vhodná" technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající riziku. Vhodnost opatření se neposuzuje podle toho, "co aplikace říká, že dělá", ale podle skutečného rizika. Pokud data klienta skončí na serveru, jehož jurisdikce nezaručuje úroveň ochrany odpovídající Evropskému hospodářskému prostoru, správce údajů – tedy profesionál – podstupuje riziko, kterého si pravděpodobně není plně vědom.

A není to jen GDPR. Profesní tajemství, upravené specificky pro advokáty, lékaře, psychology, auditory, novináře a další, vyžaduje, aby komunikace s klientem byla důvěrná. Nikoliv "důvěrná v rámci možností". Důvěrná bez výhrad. Pokud použitý technický kanál toto nemůže zaručit, profesionál podstupuje riziko, které mu etika jeho povolání nedovoluje podstoupit.

Paradoxem je, že riziko je neviditelné. Nikdo neauditu je messaging v kanceláři. Nikdo nežádá o smlouvu o zpracování údajů od poskytovatele chatu. Riziko se vynoří, až když je pozdě: únik, zveřejněné narušení bezpečnosti, soudní příkaz vykonaný na jiném kontinentu bez oznámení uživateli.

Co profesionál technicky potřebuje

To, co profesionál s povinností mlčenlivosti potřebuje, je z hlediska požadavků ve skutečnosti překvapivě jednoduché:

- Kanál, kde zprávy putují přímo ze zařízení odesílatele do zařízení příjemce, aniž by procházely přes zprostředkující server, který ukládá kopie.
- Infrastrukturu, jejíž jurisdikce a politika jsou v souladu s GDPR již z principu návrhu, nikoli jen prohlášením.
- Způsob identifikace s protějškem, aniž by bylo nutné předávat třetí straně profesní kontakty (jména klientů, telefonní čísla, seznam kontaktů).
- Ověřitelný systém – nikoli založený na slově poskytovatele – pro potvrzení, že zpráva dorazila správné osobě.

Není to náročný seznam. Je to ve skutečnosti to, co se v předdigitální profesionální komunikaci považovalo za samozřejmé. Doporučený dopis splňoval všechna tato kritéria. Telefonní hovor z ústředny kanceláře k ústředně klienta rovněž. Zvláštní není to, že tyto záruky jsou vyžadovány dnes: zvláštní je, že se ztratily při přechodu na digitální kanál, aniž by si toho kdokoli všiml.

Rozdíl mezi šifrováním a neukládáním

Existuje užitečná metafora. Zašifrovat zprávu a uložit ji na server je ekvivalentní vložení dokumentu do trezoru a ponechání trezoru v domě cizího člověka. Trezor je dobrý. Dokument v principu nelze přečíst. Dokument však *stále zůstává v domě někoho jiného*. A tento někdo může obdržet soudní příkaz, může utrpět kybernetický útok, může změnit své servisní podmínky, může být koupen jinou společností s jinou etikou nebo může zítra zmizet.

Strukturální alternativou – nikoli procedurální, nikoli založenou na důvěře – je, že dokument nikdy neopustí kancelář. Že putuje přímo od stolu profesionála ke stolu klienta bez jakéhokoli zprostředkovatele. To je to, co technicky dělá point-to-point komunikace mezi zařízeními: odstraňuje zprostředkovatele. Nejde o to, že by zprostředkovatel byl špatný. Jde o to, že v případě profesního tajemství je zprostředkovatel *zbytečný*. A to, co je zbytečné, musí být v každém systému, který aspiruje na bezpečnost, z principu odstraněno.

Otázka odpovědnosti

Nakonec otázka, na kterou by měl být schopen každý profesionál s povinností mlčenlivosti odpovědět rázné ano, zní následovně:

> Pokud by zítra unikla konverzace s jedním z mých klientů a soud nebo profesní komora by se mě zeptaly, jak spravuji důvěrnost, mohu technicky prokázat, že kanál, který jsem použil, neukládá kopie v infrastruktuře třetích stran? Mohu dokázat, že data nikdy neopustila zařízení dvou osob, které se konverzace účastnily? Mohu bez závislosti na slově společnosti z jiného kontinentu dokázat, že důvěrnost byla zaručena architekturou, a nikoli slibem?

Pokud je odpověď ne, problémem není konkrétní nástroj. Problémem je, že na nástroj byla delegována odpovědnost, pro jejíž podporu nebyl nástroj navržen. Je to jako vkládat důvěrné spisy do průhledné obálky a věřit, že se pošťák nepodívá.

Nástroj, který si profesionál vybere ke komunikaci se svými klienty, vypovídá mnohé o tom, jak si cení jejich důvěry. Existují nástroje navržené tak, aby tato důvěra nezávisela na slibech, ale na architektuře. A existují nástroje, které takové nejsou. Znát rozdíl je součástí práce.

Poznámka redakce: Pokud tyto Cuadernos zmiňují firmy nebo produkty, není to za účelem obviňování. Ti, kteří je vytvářejí, odvádějí práci, kterou miliony lidí používají a oceňují. To, na co poukazujeme, je strukturální — model, nikoliv značka. Značky uvádíme jako příklad, protože jsou pro čtenáře rozpoznatelné.

Citovaný právní rámec

- Nařízení EU 2016/679 (GDPR), zejména čl. 5, 25 (záměrná a nezbytná ochrana údajů) a 32 (zabezpečení zpracování).
- Zákon č. 85/1996 Sb., o advokacii, § 21 (povinnost mlčenlivosti advokáta).
- Zákon č. 372/2011 Sb., o zdravotních službách, § 51 (povinnost mlčenlivosti zdravotnického pracovníka).
- Etický kodex České advokátní komory ohledně důvěrnosti a profesního tajemství.

← PředchozíŠifrovat neznamená být v soukromí: co o vás vypovídají metadataDalší →GDPR a profesionální messaging: proč většina porušuje předpisy, aniž by o tom věděla

Nedávné čtení

- Analýza · 18. května 2026 Skutečné vs. zdánlivé soukromí: otázky, které je vhodné si položit
- Analýza · 18. května 2026 Self-hosting jako profesionální praxe
- Koncept · 18. května 2026 24 slov: co je to kryptografická identita

Vezměte si tento článek tam, kam potřebujete.

↓ Markdown ↓ Prostý text ↓ PDF

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 a96ee6ad8df172f7a65539a50e5cb752291d130fc40f0ead7961555772d6e1ac

Cuadernos Lacre · Publikace Menzuri Gestión S.L. ·
napsal R.Eugenio · rediguje tým Solo2.

Tento web nepoužívá cookies a nenačítá zdroje třetích stran. Používá anonymní počítadlo návštěv (Umami, na našem evropském serveru) a minimální nezbytný JavaScript pro dva ovládací prvky v záhlaví: světlý nebo tmavý motiv a výběr jazyka. Bez trackerů, bez profilování, bez sdílení dat. Pokud nás chcete sledovat: RSS.