

Profesijné tajomstvo v digitálnej ére

Ak komunikácia medzi profesionálom a jeho klientom prebieha technicky nevhodným kanálom, tajomstvo sa neporuší v deň úniku. Bolo porušené oveľa skôr, v okamihu výberu nástroja.

Problém, ktorý takmer nikto nevidí

Advokát dostane na svoj telefón citlivý dokument od klienta. Lekár konzultuje s kolegom chúlóstivú diagnózu. Psychológ koordinuje s psychiatrom liečbu pacienta. Daňový poradca zasiela údaje z priznania čakajúceho na revíziu. Všetci tak robia prostredníctvom instant messagingu. A takmer nikto sa nezastaví, aby sa zamyslel nad tým, kde tieto správy skutočne končia.

Odpoveď je vo väčšine prípadov rovnaká: na serveri, ktorý profesionál nekontroluje, v krajine, ktorej legislatívu nemusí nutne poznať, spravovanom spoločnosťou, ktorej obchodným modelom je – vyjadrené priamymi ekonomickými termínmi – hromadenie údajov. Správa môže byť pri prenose šifrovaná. Akonáhle však dorazí na server, je to kópia uložená v infraštruktúre tretej strany, ktorá podlieha operatívnym, právnym a komerčným rozhodnutiam tejto tretej strany. Nie profesionála.

Čo hovorí legislatíva

Európske všeobecné nariadenie o ochrane údajov je vo svojom článku 32 jednoznačné: ktokoľvek spracúva osobné údaje, musí uplatniť "vhodné" technické a organizačné opatrenia, aby zaistil úroveň bezpečnosti zodpovedajúcu riziku. Vhodnosť opatrení sa neposudzuje podľa toho, "čo aplikácia hovorí, že robí", ale podľa skutočného rizika. Ak údaje klienta skončia na serveri, ktorého jurisdikcia nezaručuje úroveň ochrany zodpovedajúcu Európskemu hospodárskemu priestoru, prevádzkovateľ – teda profesionál – podstupuje riziko, ktorého si pravdepodobne nie je plne vedomý.

A nie je to len GDPR. Profesijné tajomstvo, upravené špecificky pre advokátov, lekárov, psychológov, audítorov, novinárov a ďalších, vyžaduje, aby komunikácia s klientom bola dôverná. Nie "dôverná v rámci možností". Dôverná bez výhrad. Ak použitý technický kanál toto nemôže zaručiť, profesionál podstupuje riziko, ktoré mu etika jeho povolania nedovoľuje podstupiť.

Paradoxom je, že riziko je neviditeľné. Nikto neaudituje messaging v kancelárii. Nikto nežiada o zmluvu o spracúvaní údajov od poskytovateľa chatu. Riziko sa vynorí, až keď je neskoro: únik, zverejnené narušenie bezpečnosti, súdny príkaz vykonaný na inom kontinente bez oznámenia používateľovi.

Čo profesionál technicky potrebuje

To, čo profesionál s povinnosťou mlčanlivosti potrebuje, je z hľadiska požiadaviek v skutočnosti prekvapivo jednoduché:

- Kanál, kde správy putujú priamo zo zariadenia odosielateľa do zariadenia príjemcu, bez toho, aby prechádzali cez sprostredkujúci server, ktorý ukladá kópie.

- Infraštruktúru, ktorej jurisdikcia a politika sú v súlade s GDPR už z princípu návrhu, nie len vyhlásením.
- Spôsob identifikácie s protistranou bez toho, aby bolo nutné odovzdávať tretej strane profesijné kontakty (mená klientov, telefónne čísla, zoznam kontaktov).
- Overiteľný systém – nie založený na slove poskytovateľa – na potvrdenie, že správa dorazila správnej osobe.

Nie je to náročný zoznam. Je to v skutočnosti to, čo sa v preddigitálnej profesionálnej komunikácii považovalo za samozrejmosť. Doporučený list spĺňal všetky tieto kritériá. Telefónny hovor z ústredne kancelárie k ústredni klienta takisto. Zvlášť nie je to, že tieto záruky sú vyžadované dnes: zvlášť je, že sa stratili pri prechode na digitálny kanál bez toho, aby si to ktokoľvek všimol.

Rozdiel medzi šifrovaním a neukladaním

Existuje užitočná metafora. Zašifrovať správu a uložiť ju na server je ekvivalentné vloženiu dokumentu do trezoru a ponechaniu trezoru v dome cudzieho človeka. Trezor je dobrý. Dokument v princípe nie je možné prečítať. Dokument však *stále zostáva v dome niekoho iného*. A tento niekto môže dostať súdny príkaz, môže utrpieť kybernetický útok, môže zmeniť svoje servisné podmienky, môže byť kúpený inou spoločnosťou s inou etikou alebo môže zajtra zmiznúť.

Štruktúrnou alternatívou – nie procedurálnou, nie založenou na dôvere – je, že dokument nikdy neopustí kanceláriu. Že putuje priamo od stola profesionála k stolu klienta bez akéhokoľvek sprostredkovateľa. To je to, čo technicky robí point-to-point komunikácia medzi zariadeniami: odstraňuje sprostredkovateľa. Nejde o to, že by sprostredkovateľ bol zlý. Ide o to, že v prípade profesijného tajomstva je sprostredkovateľ *zbytočný*. A to, čo je zbytočné, musí byť v každom systéme, ktorý aspiruje na bezpečnosť, z princípu odstránené.

Otázka zodpovednosti

Nakoniec otázka, na ktorú by mal byť schopný každý profesionál s povinnosťou mlčanlivosti odpovedať rázne áno, znie nasledovne:

Ak by zajtra unikla konverzácia s jedným z mojich klientov a súd alebo profesijná komora by sa ma spýtali, ako spravujem dôvernosť, môžem technicky preukázať, že kanál, ktorý som použil, neukladá kópie v infraštruktúre tretích strán? Môžem dokázať, že údaje nikdy neopustili zariadenia dvoch osôb, ktoré sa konverzácie zúčastnili? Môžem bez závislosti na slove spoločnosti z iného kontinentu dokázať, že dôvernosť bola zaručená architektúrou, a nie sľubom?

Ak je odpoveď nie, problémom nie je konkrétny nástroj. Problémom je, že na nástroj bola delegovaná zodpovednosť, pre ktorej podporu nebol nástroj navrhnutý. Je to ako vkladať dôverné spisy do priehľadnej obálky a veriť, že sa poštár nepozrie.

Nástroj, ktorý si profesionál vyberie na komunikáciu so svojimi klientmi, vypovedá mnohé o tom, ako si cení ich dôveru. Existujú nástroje navrhnuté tak, aby táto dôvera nezávisela na sľuboch, ale na architektúre. A existujú nástroje, ktoré také nie sú. Poznať rozdiel je súčasťou práce.

Citovaný právny rámec

- Nariadenie EÚ 2016/679 (GDPR), najmä čl. 5, 25 (zámerná a nevyhnutná ochrana údajov) a 32 (bezpečnosť spracúvania).
- Zákon č. 586/2003 Z. z. o advokácii, § 18 (povinnosť mlčanlivosti advokáta).
- Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, § 80 (povinnosť mlčanlivosti zdravotníckeho pracovníka).
- Etické kódexy profesijných komôr týkajúce sa dôvernosti a profesijného tajomstva.

[← Predchádzajúci](#)Šifrovať neznamená byť v súkromí: čo o vás vypovedajú metadátaNasledujúci [→ GDPR a profesionálny messaging: prečo väčšina porušuje predpisy bez toho, aby o tom vedela](#)

Nedávne čítanie

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Vezmite si tento článok tam, kam potrebujete.

[↓ Markdown](#) [↓ Čistý text](#) [↓ PDF](#)

Súbor sa stiahne do vášho zariadenia. Odtiaľ si ho môžete uložiť, importovať do Solo2 alebo zdieľať, kdekoľvek chcete. Cuadernos za vás o ciele nerozhoduje.

Vosková pečať · SHA-256 41c5fa514a9da57074318927ebf438b4dc095e8c966269f719a37583667b43d0

Cuadernos Lacre · Publikácia spoločnosti [Menzuri Gestión S.L.](#) ·
napísal R.Eugenio · edituje tím [Solo2](#).

Tento web nepoužíva súbory cookie a nenačítava zdroje tretích strán. Používa anonymné počítadlo návštev s vlastným hostingom (Umami, na našom európskom serveri) a minimálne množstvo JavaScriptu nevyhnutné pre vašu preferenciu svetlého/tmavého motívu. Žiadne trackery, žiadne profilovanie, žiadne zdieľanie údajov. Ak nás chcete sledovať: [RSS](#).