GDPR a profesionální messaging: proč většina porušuje předpisy, aniž by o tom věděla

Téměř každá kancelář, ordinace nebo poradenská firma zasílá dokumenty s klientskými údaji prostřednictvím aplikací, jejichž server se nachází mimo Evropský hospodářský prostor. Bez zlého úmyslu, ale v mnoha případech v rozporu s nařízením, aniž by je na to kdokoli upozornil.

Dokument, který putuje více, než si myslíte

Každodenní situace: daňová poradkyně obdrží přes messaging dokument s údaji klienta. Obchodník přepošle přes chat nabídku kolegovi. Lékařka sdílí stejnou cestou klinickou zprávu s kolegou. Nikdo o tom nepřemýšlí dvakrát. Je to normální. Je to pohodlné. Je to to, co se děje každý den v každé kanceláři v každém městě v Evropě.

Tento dokument však v mnoha případech právě doputoval na server ve Spojených státech. Byl uložen – byť dočasně, byť "šifrovaně v klidu" – v cloudu, který ani profesionál, ani jeho klient nekontrolují. Prošel systémy, které technicky mohou indexovat metadata spojená s obsahem. A evropské obecné nařízení o ochraně osobních údajů k tomu má co říct docela jasně.

Co předpisy vyžadují

GDPR – a v návaznosti na něj judikatura Soudního dvora Evropské unie (zejména rozsudek Schrems II, C-311/18, z roku 2020) – stanovuje, že osobní údaje evropských občanů musí být adekvátně chráněny. Pokud tyto údaje opouštějí Evropský hospodářský prostor, musí správce údajů zaručit, že příjemce nabízí úroveň ochrany "v zásadě rovnocennou" té evropské. V praxi to znamená, že zasílání klientských údajů prostřednictvím služeb, jejichž servery podléhají jurisdikci USA, aniž by bylo provedeno posouzení dopadů a zavedeny doplňkové záruky – standardní smluvní doložky, dodatečná technická opatření jako ověřitelné šifrování atd. – může představovat porušení nařízení. I když zatím nikdo nic neřekl.

A nejde jen o obsah zpráv. Metadata – kdo co komu posílá, kdy, jak často, odkud – jsou podle předpisů a podle opakovaného výkladu Evropského sboru pro ochranu osobních údajů rovněž osobními údaji. Služba, která sbírá metadata z profesionální komunikace uživatele, zpracovává osobní údaje klientů tohoto uživatele, aniž by o tom tito věděli nebo k takovému zpracování udělili jakýkoli souhlas.

Běžné myšlenkové schéma – "používám aplikaci jen k psaní; aplikace není dodavatelem údajů mého klienta" – je právně nesprávné. Pokud data klienta procházejí infrastrukturou třetí strany, tato třetí strana tato data zpracovává. A pokud je zpracovává, musí existovat právní základ, smlouva o zpracování údajů a odpovídající záruky.

Kdo je odpovědný

Otázka, kdo nese právní odpovědnost, není akademická. GDPR rozlišuje mezi *správcem údajů* (kdo rozhoduje o tom, jaká data se zpracovávají a za jakým účelem) a *zpracovatelem údajů* (kdo tak činí fakticky, jménem správce). Profesionál, který zasílá klientské dokumenty, je správcem. Poskytovatel messagingové aplikace je v mnoha případech faktickým zpracovatelem. Bez smlouvy o zpracování – a bez většiny doložek, které by taková smlouva měla obsahovat – správce nesplnil svou povinnost.

Mírný výklad zní: "většina profesionálů o tom neví". Přísný výklad zní: "neznalost zákona neomlouvá". A výklad jakéhokoli právníka specializovaného na ochranu údajů, který je v této věci konzultován, je zpravidla ten přísný.

Pro koho je toto konkrétně důležité

Pro každého profesionála nebo firmu, která byť jen příležitostně nakládá s osobními údaji třetích stran:

- Advokáti, kteří přijímají dokumentaci od klientů (smlouvy, žaloby, prohlášení, majetkové zprávy).
- Lékaři a další zdravotničtí pracovníci, kteří sdílejí údaje o zdravotním stavu – považované podle čl. 9 GDPR za *zvláštní kategorii* se zpřísněným režimem ochrany –.
- Daňoví poradci a administrativní správci, kteří nakládají s identifikačními, daňovými a bankovními údaji.
- Oddělení lidských zdrojů, která spravují pracovní a osobní dokumentaci zaměstnanců.
- Obchodníci, kteří přijímají kontaktní údaje a často citlivé obchodní informace od potenciálních i stávajících klientů.

Ve všech případech jsou informace chráněny GDPR. Ve všech případech v běžné praxi tyto informace procházejí kanály, jejichž jurisdikce neumožňuje jejich prohlášení za "v zásadě rovnocenné" evropskému rámci bez dodatečných záruk. Nikoliv ze zlého úmyslu. Ze zvyku. A kvůli technologické infrastruktuře, která po patnáct let upřednostňovala pohodlí před dodržováním předpisů.

Argument "každý to tak dělá"

Je vhodné předjímat nejčastější námitku: "pokud to dělají všichni, nemůže to být skutečný problém". Je to naprosto pochopitelný argument a právně nemá žádnou váhu. Skutečnost, že je nějaká praxe rozšířená, ji nečiní v souladu s nařízením. Úřady pro ochranu osobních údajů (v ČR ÚOOÚ) v posledních letech sankcionovaly několik firem právě za způsoby používání messagingu, které se do okamžiku kontroly zdály neškodné.

Současná operativní realita je taková, že riziko je nízké z hlediska pravděpodobnosti – je velmi vzácné, aby kontrola Úřadu auditovala konkrétní messagingové nástroje středně velké kanceláře –, ale vysoké z hlediska dopadu, pokud se zhmotní. Je to riziko, které většina podstupuje, aniž by věděla, že ho podstupuje. Tedy aniž by posoudila, zda je použitý nástroj v souladu s právní odpovědností správce údajů.

Digitální stopa je retroaktivní

Existuje druhý argument, téměř symetrický k předchozímu, který je vhodné předjímat: *"kdyby to byl vážný problém, správa by ho už začala kontrolovat"*. Současná pozorovaná realita mu dává povrchně za pravdu. Kontroly kvůli nevhodnému používání messagingu v malých firmách a zejména u živnostníků jsou dnes téměř neexistující – nikoli proto, že by takové jednání bylo dovoleno, ale proto, že správě v ČR i ve velké části EU chybí lidské zdroje potřebné k auditu milionů povinných subjektů.

To je to, co naznačuje dnešní pozorovaná praxe. Není to to, co naznačuje příští desetiletí. Dva vektory se sbíhají, aby změnily rovnováhu v relativně krátkých lhůtách.

Za prvé: digitální stopa je retroaktivní. Každá zpráva odeslaná prostřednictvím aplikace s centrálním serverem zůstává zaznamenána – alespoň v metadatech – v infrastruktuře, která přetrvává. To, co bylo odesláno před šesti měsíci, je technicky stále auditovatelné dnes. To, co bude odesláno dnes, bude auditovatelné i za pět

let. Absence současné kontroly není zárukou absence budoucí kontroly. Je to odklad posouzení, nikoli osvobození.

Za druhé: kapacita správního auditu poroste zrychleným tempem. Zavedení nástrojů umělé inteligence do kontrolních procesů odstraňuje lidské úzké hrdlo, které dosud chránilo – fakticky, nikoli právně – malé firmy a živnostníky. Systém schopný křížově porovnávat masivní metadata, daňová přiznání, obchodní rejstříky a povinnosti oznamovat narušení bezpečnosti nevyžaduje inspektory: vyžaduje přístup. A přístup je prostřednictvím požadavků na poskytovatele s právní přítomností v EU v rámci současného normativního rámce naprosto proveditelný.

K tomu se přidává faktor méně technický, ale stejně určující: evropské státy jsou v procesu trvalého rostoucího zadlužování a potřebují téměř bez výjimky rozšířit svou daňovou základnu. Správní sankce vyplývající z nedodržení GDPR je v čistě fiskálních termínech rostoucím a politicky pohodlným zdrojem příjmů. Není to domněnka: je to pozorovatelný trend ve výročních zprávách evropských úřadů pro ochranu osobních údajů, kde celkový objem sankcí roste již několik po sobě jdoucích účetních období.

Operativní závěr pro správce údajů není alarmistický, ale chladný: **rozhodnutí o tom, jak se dnes spravuje komunikace s klienty, se posuzuje podle kontrolní kapacity roku, ve kterém kontrola dorazí, nikoli podle té současné.** A tato kapacita bude v přiměřených lhůtách podstatně jiná než dnes. Kdo začne dělat věci správně dnes, nebude v pořádku jen od dneška: stopa generovaná od tohoto okamžiku bude v souladu s předpisy, a to zpětně chrání nadcházející úsek. Kdo bude pokračovat jako dosud, bude hromadit auditovatelnou stopu, jejíž shoda bude posuzována podle standardů – a zdrojů – příštích let.

Co se mění s odlišnou architekturou

Existují technické alternativy, u nichž se data neukládají v infrastruktuře třetích stran, ale putují přímo ze zařízení odesílatele do zařízení příjemce. V této architektuře dodržování GDPR s ohledem na mezinárodní předávání údajů nezávisí na standardních smluvních doložkách, ani na dobré vůli poskytovatele, ani na budoucích auditech. Závisí na tom, že *nedochází k předávání*. A to, co neexistuje, nelze porušit.

Toto není exkluzivní řešení ani jediné možné. Je však strukturálně odlišné a dodržování předpisů přestává být procedurálním doplňkem a stává se přímým důsledkem návrhu. Pro profesionála, který bere svou odpovědnost správce údajů vážně, na tomto rozdílu záleží.

Příští vydání Cuadernos podrobně analyzuje rozsudek Schrems II a jeho praktické dopady pro malé a střední firmy závislé na amerických cloudových službách, pět let po jeho zveřejnění.

Zdroje a právní rámec

- Nařízení EU 2016/679 (GDPR), zejména kapitola V o mezinárodním předávání.
- SDEU C-311/18 ("Schrems II"), 16. července 2020.
- EDPB – Doporučení 01/2020 k opatřením, která doplňují nástroje předávání.
- ÚOOÚ (a další dozorové úřady) – Výroční zprávy s kazuistikou sankcí za nevhodné používání instant messagingu v profesním prostředí.

← PředchozíProfesní tajemství v digitální éřeDalší →Když není nikdo uprostřed

Nedávné čtení

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 55f5776cdff2e2cd4323840a2ec229f94c3ed06e902461f630e82435daa97214

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