GDPR a profesionálny messaging: prečo väčšina porušuje predpisy bez toho, aby o tom vedela

Takmer každá kancelária, ordinácia alebo poradenská firma zasiela klientske dokumenty prostredníctvom aplikácií, ktorých server sa nachádza mimo Európskeho hospodárskeho priestoru. Bez zlého úmyslu, ale v mnohých prípadoch v rozpore s nariadením bez toho, aby ich na to niekto upozornil.

Dokument, ktorý putuje viac, než si myslíte

Každodenná situácia: daňová poradkyňa dostane cez messaging dokument s údajmi klienta. Obchodník prepošle cez chat ponuku kolegovi. Lekárka zdieľa rovnakou cestou klinickú správu s kolegom. Nikto o tom nepremýšľa dvakrát. Je to normálne. Je to pohodlné. Je to to, čo sa deje každý deň v každej kancelárii v každom meste v Európe.

Tento dokument však v mnohých prípadoch práve doputoval na server v Spojených štátoch. Bol uložený – hoci dočasne, hoci "šifrovane v pokoji" – v cloude, ktorý ani profesionál, ani jeho klient nekontrolujú. Prešiel systémami, ktoré technicky môžu indexovať metadáta spojené s obsahom. A európske všeobecné nariadenie o ochrane údajov má k tomu čo povedať celkom jasne.

Čo predpisy vyžadujú

GDPR – a v nadväznosti naň judikatúra Súdneho dvora Európskej únie (najmä rozsudok Schrems II, C-311/18, z roku 2020) – stanovuje, že osobné údaje európskych občanov musia byť adekvátne chránené. Ak tieto údaje opúšťajú Európsky hospodársky priestor, prevádzkovateľ musí zaručiť, že príjemca ponúka úroveň ochrany "v zásade rovnocennú" tej európskej. V praxi to znamená, že zasielanie klientskych údajov prostredníctvom služieb, ktorých servery podliehajú jurisdikcii USA, bez vykonania posúdenia vplyvu a zavedenia doplnkových záruk – štandardných zmluvných doložiek, dodatočných technických opatrení ako overiteľné šifrovanie atď. – môže predstavovať porušenie nariadenia. Aj keď zatiaľ nikto nič nepovedal.

A nejde len o obsah správ. Metadáta – kto čo komu posiela, kedy, ako často, odkiaľ – sú podľa predpisov a podľa opakovanej interpretácie Európskeho výboru pre ochranu údajov rovnako osobnými údajmi. Služba, ktorá zbiera metadáta z profesionálnej komunikácie používateľa, spracúva osobné údaje klientov tohto používateľa bez toho, aby o tom títo vedeli alebo k takému spracúvaniu udelili akýkoľvek súhlas.

Bežná myšlienková schéma – "používam aplikáciu len na písanie; aplikácia nie je dodávateľom údajov môjho klienta" – je právne nesprávna. Ak údaje klienta prechádzajú infraštruktúrou tretej strany, táto tretia strana tieto údaje spracúva. A ak ich spracúva, musí existovať právny základ, zmluva o spracúvaní údajov a zodpovedajúce záruky.

Kto je zodpovedný

Otázka, kto nesie právnu zodpovednosť, nie je akademická. GDPR rozlišuje medzi *prevádzkovateľom* (kto rozhoduje o tom, aké údaje sa spracúvajú a na aký účel) a *sprostredkovateľom* (kto tak robí fakticky, v mene prevádzkovateľa). Profesionál, ktorý zasiela klientske dokumenty, je prevádzkovateľom. Poskytovateľ messagingovej aplikácie je v mnohých prípadoch faktickým sprostredkovateľom. Bez zmluvy o spracúvaní – a bez väčšiny doložiek, ktoré by takáto zmluva mala obsahovať – prevádzkovateľ nesplnil svoju povinnosť.

Mierny výklad znie: "väčšina profesionálov o tom nevie". Prísny výklad znie: "neznalosť zákona neospravedlňuje". A výklad akéhokoľvek právnika špecializovaného na ochranu údajov, ktorý je v tejto veci konzultovaný, je spravidla ten prísny.

Pre koho je toto konkrétne dôležité

Pre každého profesionála alebo firmu, ktorá hoci len príležitostne narába s osobnými údajmi tretích strán:

- Advokáti, ktorí prijímajú dokumentáciu od klientov (zmluvy, žaloby, vyhlásenia, majetkové správy).
- Lekári a ďalší zdravotnícki pracovníci, ktorí zdieľajú údaje o zdravotnom stave – považované podľa čl. 9 GDPR za *osobitnú kategóriu* so sprísneným režimom ochrany –.
- Daňoví poradcovia a administratívni správcovia, ktorí narábajú s identifikačnými, daňovými a bankovými údajmi.
- Oddelenia ľudských zdrojov, ktoré spravujú pracovnú a osobnú dokumentáciu zamestnancov.
- Obchodníci, ktorí prijímajú kontaktné údaje a často citlivé obchodné informácie od potenciálnych aj existujúcich klientov.

Vo všetkých prípadoch sú informácie chránené GDPR. Vo všetkých prípadoch v bežnej praxi tieto informácie prechádzajú kanálmi, ktorých jurisdikcia neumožňuje ich vyhlásenie za "v zásade rovnocenné" európskemu rámcu bez dodatočných záruk. Nie zo zlého úmyslu. Zo zvyku. A kvôli technologickej infraštruktúre, ktorá po pätnásť rokov uprednostňovala pohodlie pred dodržiavaním predpisov.

Argument "každý to tak robí"

Je vhodné predvídať najčastejšiu námietku: "ak to robia všetci, nemôže to byť skutočný problém". Je to naprosto pochopiteľný argument a právne nemá žiadnu váhu. Skutočnosť, že je nejaká prax rozšírená, ju nerobí v súlade s nariadením. Úrady na ochranu osobných údajov v posledných rokoch sankcionovali niekoľko firiem práve za spôsoby používania messagingu, ktoré sa do okamihu kontroly zdali neškodné.

Súčasná operatívna realita je taká, že riziko je nízke z hľadiska pravdepodobnosti – je veľmi vzácne, aby kontrola Úradu auditovala konkrétne messagingové nástroje stredne veľkej kancelárie –, ale vysoké z hľadiska dopadu, ak sa zhmotní. Je to riziko, ktoré väčšina podstupuje bez toho, aby vedela, že ho podstupuje. Teda bez posúdenia, či je použitý nástroj v súlade s právnou zodpovednosťou prevádzkovateľa.

Digitálna stopa je retroaktívna

Existuje druhý argument, takmer symetrický k predchádzajúcemu, ktorý je vhodné predvídať: *"keby to bol vážny problém, správa by ho už začala kontrolovať"*. Súčasná pozorovaná realita mu dáva povrchne za pravdu. Kontroly kvôli nevhodnému používaniu messagingu v malých firmách a najmä u živnostníkov sú dnes takmer neexistujúce – nie preto, že by také konanie bolo dovolené, ale preto, že správe vo veľkej časti EU chýbajú ľudské zdroje potrebné na audit miliónov povinných subjektov.

To naznačuje dnešná pozorovaná prax. Nie je to to, čo naznačuje budúce desaťročie. Dva vektory sa zbiehajú, aby zmenili rovnováhu v relatívne krátkych lehotách.

Po prvé: digitálna stopa je retroaktívna. Každá správa odoslaná prostredníctvom aplikácie s centrálnym serverom zostáva zaznamenaná – aspoň v metadátach – v infraštruktúre, ktorá pretrváva. To, čo bolo odoslané

pred šiestimi mesiacmi, je technicky stále auditovateľné dnes. To, čo bude odoslané dnes, bude auditovateľné aj o päť rokov. Absencia súčasnej kontroly nie je zárukou absencie budúcej kontroly. Je to odklad posúdenia, nie oslobodenie.

Po druhé: kapacita správneho auditu porastie zrýchleným tempom. Zavedenie nástrojov umelej inteligencie do kontrolných procesov odstraňuje ľudské úzke hrdlo, ktoré doteraz chránilo – fakticky, nie právne – malé firmy a živnostníkov. Systém schopný krížovo porovnávať masívne metadáta, daňové priznania, obchodné registre a povinnosti oznamovať narušenia bezpečnosti nevyžaduje inšpektorov: vyžaduje prístup. A prístup je prostredníctvom požiadaviek na poskytovateľov s právnou prítomnosťou v EÚ v rámci súčasného normatívneho rámca naprosto uskutočniteľný.

K tomu sa pridáva faktor menej technický, ale rovnako určujúci: európske štáty sú v procese trvalého rastúceho zadlžovania a potrebujú takmer bez výnimky rozšíriť svoju daňovú základňu. Správna sankcia vyplývajúca z nedodržania GDPR je v čisto fiskálnych termínoch rastúcim a politicky pohodlným zdrojom príjmov. Nie je to domnienka: je to pozorovateľný trend vo výročných správach európskych úradov na ochranu osobných údajov, kde celkový objem sankcií rastie už niekoľko po sebe idúcich účtovných období.

Operatívny záver pre prevádzkovateľa nie je alarmistický, ale chladný: **rozhodnutie o tom, ako sa dnes spravuje komunikácia s klientmi, sa posudzuje podľa kontrolnej kapacity roku, v ktorom kontrola dorazí, nie podľa tej súčasnej.** A táto kapacita bude v primeraných lehotách podstatne iná než dnes. Kto začne robiť veci správne dnes, nebude v poriadku len od dneška: stopa generovaná od tohto okamihu bude v súlade s predpismi, a to spätne chráni nadchádzajúci úsek. Kto bude pokračovať ako doteraz, bude hromadiť auditovateľnú stopu, ktorej zhoda bude posudzovaná podľa štandardov – a zdrojov – budúcich rokov.

Čo sa mení s odlišnou architektúrou

Existujú technické alternatívy, pri ktorých sa údaje neukladajú v infraštruktúre tretích strán, ale putujú priamo zo zariadenia odosielateľa do zariadenia príjemcu. V tejto architektúre dodržiavanie GDPR s ohľadom na medzinárodné prenosy údajov nezávisí od štandardných zmluvných doložiek, ani od dobrej vôle poskytovateľa, ani od budúcich auditov. Závisí od toho, že *nedochádza k prenosu*. A to, čo neexistuje, nemožno porušiť.

Toto nie je exkluzívne riešenie ani jediné možné. Je však štrukturálne odlišné a dodržiavanie predpisov prestáva byť procedurálnym doplnkom a stáva sa priamym dôsledkom návrhu. Pre profesionála, ktorý berie svoju zodpovednosť prevádzkovateľa vážne, na tomto rozdiele záleží.

Budúce vydanie Cuadernos podrobne analyzuje rozsudok Schrems II a jeho praktické dopady pre malé a stredné firmy závislé na amerických cloudových službách, päť rokov po jeho zverejnení.

Zdroje a právny rámec

- Nariadenie EÚ 2016/679 (GDPR), najmä kapitola V o medzinárodnom prenose.
- SDEÚ C-311/18 ("Schrems II"), 16. júla 2020.
- EDPB – Odporúčania 01/2020 k opatreniam, ktoré dopĺňajú nástroje prenosu.
- ÚOOÚ SR (a ďalšie dozorné úrady) – Výročné správy s kazuistikou sankcií za nevhodné používanie instant messagingu v profesijnom prostredí.

← PredchádzajúciProfesijné tajomstvo v digitálnej éreNasledujúci →Keď v strede nikto nie je

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 cieli nerozhoduje.

Vosková pečať · SHA-256 aa0da7fe512cc1a431d2861ecf74d18c8fe1141d9762c45c920f62ee2b304715

Cuadernos Lacre · Publikácia spoločnosti Menzuri Gestión S.L. ·
napísal R.Eugenio · edituje tím Solo2.