Analiza · 16. svibnja 2026

← Prethodno·Sljedeće →

GDPR i profesionalna razmjena poruka: zašto većina krši pravila, a da to i ne zna

Gotovo svaki ured, ordinacija ili savjetodavna tvrtka šalje klijentske dokumente putem aplikacija čiji se poslužitelj nalazi izvan Europskog gospodarskog prostora. Bez loše namjere, ali u mnogim slučajevima kršeći uredbu, a da ih na to nitko nije upozorio.

Dokument koji putuje više nego što mislite

Svakodnevna situacija: porezna savjetnica putem razmjene poruka prima dokument s podacima o klijentu. Prodajni predstavnik putem chata prosljeđuje ponudu kolegi. Liječnica istim putem dijeli klinički nalaz s kolegom. Nitko ne razmišlja dvaput o tome. To je normalno. To je praktično. To je ono što se radi svaki dan u svakom uredu u svakom gradu u Europi.

Ali taj je dokument u mnogim slučajevima upravo otputovao na poslužitelj u Sjedinjenim Državama. Pohranjen je – makar privremeno, makar "šifriran u mirovanju" – u oblaku koji ne kontroliraju ni profesionalac ni njegov klijent. Prošao je kroz sustave koji tehnički mogu indeksirati metapodatke povezane sa sadržajem. A europska Opća uredba o zaštiti podataka o tome ima reći nešto prilično jasno.

Što norma zahtijeva

GDPR – a posljedično i sudska praksa Suda Europske unije (posebno presuda Schrems II, C-311/18, iz 2020.) – utvrđuje da osobni podaci europskih građana moraju biti adekvatno zaštićeni. Ako ti podaci napuštaju Europski gospodarski prostor, voditelj obrade mora jamčiti da primatelj nudi razinu zaštite koja je "u bitnome istovjetna" onoj u Europi. U praksi to znači da slanje podataka o klijentima putem usluga čiji su poslužitelji pod jurisdikcijom SAD-a, bez provedene procjene učinka i implementiranih dodatnih jamstava – standardnih ugovornih klauzula, dodatnih tehničkih mjera poput provjerljive enkripcije itd. – može predstavljati kršenje uredbe. Čak i ako do sada nitko ništa nije rekao.

I ne radi se samo o sadržaju poruka. Metapodaci – tko šalje što kome, kada, koliko često, odakle – također su osobni podaci prema propisima, prema višekratnom tumačenju Europskog odbora za zaštitu podataka. Usluga koja prikuplja metapodatke iz profesionalne komunikacije korisnika obrađuje osobne podatke klijenata tog korisnika, a da oni o tome nemaju saznanja niti su dali bilo kakvu privolu za takvu obradu.

Uobičajena shema razmišljanja – "koristim aplikaciju samo za pisanje; aplikacija nije pružatelj podataka mog klijenta" – pravno je pogrešna. Ako podaci klijenta prolaze kroz infrastrukturu treće strane, ta treća strana obrađuje te podatke. A ako ih obrađuje, mora postojati pravna osnova, ugovor o obradi podataka i odgovarajuća jamstva.

Tko je odgovoran

Pitanje tko snosi pravnu odgovornost nije akademsko. GDPR razlikuje *voditelja obrade* (tko odlučuje koji se podaci obrađuju i u koju svrhu) i *izvršitelja obrade* (tko to čini materijalno u ime voditelja). Profesionalac koji šalje klijentske dokumente je voditelj obrade. Pružatelj aplikacije za razmjenu poruka je u mnogim slučajevima faktični izvršitelj obrade. Bez ugovora o obradi – i bez većine klauzula koje bi takav ugovor trebao sadržavati – voditelj nije ispunio svoju obvezu.

Blago tumačenje glasi: "većina profesionalaca to ne zna". Strogo tumačenje glasi: "nepoznavanje prava ne opravdava kršenje". A tumačenje bilo kojeg odvjetnika specijaliziranog za zaštitu podataka koji je konzultiran o tome obično je strogo.

Za koga je to konkretno važno

Za svakog profesionalca ili tvrtku koja makar povremeno operira s osobnim podacima trećih strana:

- Odvjetnici koji primaju dokumentaciju od klijenata (ugovori, tužbe, izjave, izvješća o imovini).
- Liječnici i drugi zdravstveni radnici koji dijele zdravstvene podatke – koji se prema čl. 9. GDPR-a smatraju *posebnim kategorijama* s pojačanim režimom zaštite –.
- Porezni savjetnici i administrativni upravitelji koji operiraju s identifikacijskim, poreznim i bankovnim podacima.
- Odjeli ljudskih resursa koji upravljaju radnom i osobnom dokumentacijom zaposlenika.
- Komercijalisti koji primaju kontaktne podatke i često osjetljive poslovne informacije od potencijalnih i postojećih klijenata.

U svim slučajevima informacije su zaštićene GDPR-om. U svim slučajevima u uobičajenoj praksi te informacije teku kanalima čija jurisdikcija ne dopušta njihovo proglašavanje "u bitnome istovjetnim" europskom okviru bez dodatnih jamstava. Ne iz loše namjere. Iz navike. I zbog tehnološke infrastrukture koja je petnaest godina pretpostavljala praktičnost usklađenosti.

Argument "svi to rade"

Mudro je predvidjeti najčešći prigovor: "ako svi to rade, to ne može biti stvarni problem". To je potpuno razumljiv argument i pravno nema nikakvu snagu. Činjenica da je neka praksa raširena ne čini je usklađenom s uredbom. Agencije za zaštitu podataka (poput AZOP-a u Hrvatskoj) sankcionirale su posljednjih godina nekoliko tvrtki upravo zbog načina korištenja razmjene poruka koji su se do trenutka revizije činili bezopasnim.

Trenutna operativna stvarnost je da je rizik u smislu vjerojatnosti nizak – vrlo je rijetko da nadzorno tijelo revidira specifične alate za razmjenu poruka srednje velikog ureda – ali visok u smislu učinka ako se ostvari. To je rizik koji većina prihvaća ne znajući da ga prihvaća. Odnosno, bez procjene je li korišteni alat u skladu s pravnom odgovornošću voditelja obrade.

Digitalni trag je retroaktivan

Postoji drugi argument, gotovo simetričan prethodnom, koji vrijedi predvidjeti: *"da je ovo ozbiljan problem, uprava bi to već počela kontrolirati"*. Trenutna opažena stvarnost daje mu površno za pravo. Nadzora zbog neadekvatnog korištenja razmjene poruka u malim tvrtkama, a posebno kod obrtnika, danas gotovo da i nema – ne zato što bi ponašanje bilo dopušteno, već zato što upravi u većem dijelu EU nedostaje ljudskih resursa potrebnih za reviziju milijuna obveznika.

To sugerira današnja opažena praksa. Ali to nije ono što sugerira sljedeće desetljeće. Dva vektora konvergiraju kako bi promijenila ravnotežu u relativno kratkim rokovima.

Prvo: digitalni trag je retroaktivan. Svaka poruka poslana putem aplikacije sa središnjim poslužiteljem ostaje registrirana – barem u metapodacima – u infrastrukturi koja traje. Ono što je poslano prije šest mjeseci tehnički

je i dalje podložno reviziji danas. Ono što se šalje danas bit će podložno reviziji i za pet godina. Odsutnost trenutnog nadzora nije jamstvo odsutnosti budućeg nadzora. To je odgoda procjene, a ne oslobađanje.

Drugo: kapacitet administrativne revizije rasti će ubrzano. Uvođenje alata umjetne inteligencije u procese nadzora eliminira ljudsko usko grlo koje je do sada – faktično, ne pravno – štitilo male tvrtke i obrtnike. Sustav sposoban za unakrsnu provjeru masovnih metapodataka, poreznih prijava, trgovačkih registara i obveza obavještavanja o povredama sigurnosti ne treba inspektore: treba pristup. A pristup je putem zahtjeva pružateljima s pravnom prisutnošću u EU unutar sadašnjeg normativnog okvira potpuno izvediv.

Tome se dodaje manje tehnički, ali jednako odlučujući čimbenik: europske države su u procesu stalno rastuće zaduženosti i moraju, gotovo bez iznimke, proširiti svoju poreznu osnovicu. Administrativna sankcija proizašla iz neusklađenosti s GDPR-om je u čisto fiskalnim terminima rastući i politički ugodan izvor prihoda. To nije pretpostavka: to je primjetan trend u godišnjim izvješćima europskih agencija za zaštitu podataka, gdje ukupni volumen sankcija raste već nekoliko uzastopnih fiskalnih godina.

Operativni zaključak za voditelja obrade nije alarmistički, već trijezan: **odluka o tome kako se danas upravlja komunikacijom s klijentima procjenjuje se prema kontrolnom kapacitetu godine u kojoj kontrola dođe, a ne prema trenutnom.** A taj će kapacitet u razumnom roku biti znatno drugačiji nego danas. Tko danas počne raditi stvari ispravno, neće biti u redu samo od danas: trag generiran od ovog trenutka nadalje bit će u skladu s propisima, a to retroaktivno štiti nadolazeći period. Tko nastavi kao i do sada, akumulirat će trag podložan reviziji čija će se usklađenost procjenjivati prema standardima – i resursima – budućih godina.

Što se mijenja s drugačijom arhitekturom

Postoje tehničke alternative kod kojih se podaci ne pohranjuju u infrastrukturi trećih strana, već putuju izravno s uređaja pošiljatelja na uređaj primatelja. U toj arhitekturi usklađenost s GDPR-om s obzirom na međunarodne prijenose ne ovisi o standardnim ugovornim klauzulama, niti o dobroj volji pružatelja usluge, niti o budućim revizijama. Ovisi o tome da *prijenosa nema*. A ono što ne postoji, ne može se prekršiti.

Ovo nije isključivo rješenje niti jedino moguće. Ali je strukturno drugačije i usklađenost s propisima prestaje biti proceduralni dodatak i postaje izravna posljedica dizajna. Za profesionalca koji svoju odgovornost voditelja obrade shvaća ozbiljno, ta razlika čini razliku.

Sljedeće izdanje Cuadernos detaljno će analizirati presudu Schrems II i njezine praktične implikacije za male i srednje tvrtke ovisne o američkim uslugama u oblaku, pet godina nakon njezine objave.

Izvori i pravni okvir

- Uredba (EU) 2016/679 (GDPR), posebno poglavlje V o međunarodnim prijenosima.
- Sud EU-a C-311/18 ("Schrems II"), 16. srpnja 2020.
- EDPB – Preporuke 01/2020 o mjerama koje dopunjuju alate za prijenos.
- Agencija za zaštitu osobnih podataka (AZOP) – Godišnja izvješća s kazuistikom sankcija zbog neadekvatnog korištenja trenutne razmjene poruka u profesionalnom okruženju.

← PrethodnoProfesionalna tajna u digitalnom dobuSljedeće →Kada nema nikoga u sredini

Nedavna čitanja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ponesite ovaj članak sa sobom gdje god vam zatreba.

↓ Markdown ↓ Obični tekst ↓ PDF

Datoteka će se preuzeti na vaš uređaj. Od tamo je možete spremiti, uvesti u Solo2 ili dijeliti gdje god želite. Cuadernos ne odlučuje o odredištu umjesto vas.

Voštani pečat · SHA-256 e312d4769e491585352994c1d1ec53558135783e63e3de82698d15f63db8e3dc

Cuadernos Lacre · Publikacija Menzuri Gestión S.L. ·
napisao R.Eugenio · uredio tim Solo2.