GDPR și mesageria profesională: de ce majoritatea încalcă normele fără să știe

Aproape orice birou, cabinet sau firmă de consultanță trimite documente ale clienților prin aplicații al căror server se află în afara Spațiului Economic European. Fără intenție rea, dar în multe cazuri încălcând regulamentul, fără ca cineva să-i fi avertizat.

Documentul care călătorește mai mult decât credeți

O situație cotidiană: un consultant fiscal primește prin mesagerie un document cu datele unui client. Un agent de vânzări transmite prin chat o ofertă unui coleg. Un medic partajează pe aceeași cale un raport clinic cu un coleg. Nimeni nu se gândește de două ori. Este normal. Este comod. Este ceea ce se face în fiecare zi în fiecare birou din fiecare oraș din Europa.

Dar acest document, în multe cazuri, tocmai a călătorit la un server din Statele Unite. A fost stocat – fie și temporar, fie și „criptat în repaus” – într-un cloud pe care nici profesionistul, nici clientul său nu îl controlează. A trecut prin sisteme care pot indexa tehnic metadate legate de conținut. Iar Regulamentul General European privind Protecția Datelor are ceva destul de clar de spus despre acest lucru.

Ce cere norma

GDPR – și prin extensie jurisprudența Curții de Justiție a Uniunii Europene (în special hotărârea Schrems II, C-311/18, din 2020) – stabilește că datele cu caracter personal ale cetățenilor europeni trebuie protejate în mod corespunzător. Dacă aceste date părăsesc Spațiul Economic European, operatorul trebuie să garanteze că destinatarul oferă un nivel de protecție „esențialmente echivalent” cu cel european. În practică, aceasta înseamnă că trimiterea datelor clienților prin servicii ale căror servere se află sub jurisdicția SUA, fără a fi efectuat o evaluare a impactului și fără a fi implementat garanții suplimentare – clauze contractuale standard, măsuri tehnice adiționale precum criptarea verificabilă etc. – poate constitui o încălcare a regulamentului. Chiar dacă până acum nu a spus nimeni nimic.

Și nu este vorba doar despre conținutul mesajelor. Metadatele – cine trimite ce cui, când, cât de des, de unde – sunt, de asemenea, date cu caracter personal conform normelor, conform interpretării repetate a Comitetului European pentru Protecția Datelor. Un serviciu care colectează metadate din comunicarea profesională a unui utilizator prelucrează date cu caracter personal ale clienților acelui utilizator, fără ca aceștia să aibă cunoștință sau să-și fi dat consimțământul pentru o astfel de prelucrare.

Schema de gândire obișnuită – „folosesc aplicația doar pentru a scrie; aplicația nu este furnizorul de date al clientului meu” – este eronată din punct de vedere juridic. Dacă datele clientului trec prin infrastructura unei terțe părți, acea terță parte prelucrează acele date. Și dacă le prelucrează, trebuie să existe un temei juridic, un contract de prelucrare a datelor și garanții adecvate.

Cine este responsabil

Întrebarea cine poartă responsabilitatea legală nu este academică. GDPR distinge între *operator* (cine decide ce date sunt prelucrate și în ce scop) și *persoana împuternicită de operator* (cine face acest lucru în mod material, în numele operatorului). Profesionistul care trimite documente ale clienților este operatorul. Furnizorul aplicației de mesagerie este, în multe cazuri, de fapt, persoană împuternicită. Fără un contract de împuternicire – și fără majoritatea clauzelor pe care un astfel de contract ar trebui să le conțină – operatorul nu și-a îndeplinit obligația.

Interpretarea indulgentă este: „majoritatea profesioniștilor nu știu acest lucru". Interpretarea riguroasă este: „necunoașterea legii nu scutește de respectarea ei". Iar interpretarea oricărui avocat specializat în protecția datelor care este consultat în această privință este, de regulă, cea riguroasă.

Pentru cine este acest lucru important în mod concret

Pentru orice profesionist sau companie care operează, fie și ocazional, cu informații personale ale terților:

- Avocați care primesc documentație de la clienți (contracte, cereri de chemare în judecată, declarații, rapoarte de avere).
- Medici și alți profesioniști din domeniul sănătății care partajează date privind sănătatea – care sunt considerate *categorii speciale* conform art. 9 GDPR, cu un regim de protecție sporit –.
- Consultanți fiscali și manageri administrativi care operează cu date de identificare, fiscale și bancare.
- Departamente de resurse umane care gestionează documentația de muncă și personală a angajaților.
- Agenți comerciali care primesc date de contact și adesea informații comerciale sensibile de la prospecți și clienți.

În toate cazurile, informațiile sunt protejate de GDPR. În toate cazurile, în practica obișnuită, aceste informații circulă prin canale a căror jurisdicție nu permite declararea lor ca fiind „esențialmente echivalente" cadrului european fără garanții suplimentare. Nu din rea-voință. Din obișnuință. Și din cauza unei infrastructuri tehnologice care, timp de cincisprezece ani, a pus confortul înaintea conformității.

Argumentul „toată lumea o face"

Este prudent să anticipăm cea mai frecventă obiecție: „dacă toată lumea o face, nu poate fi o problemă reală". Este un argument perfect de înțeles și nu are nicio forță din punct de vedere juridic. Faptul că o practică este răspândită nu o face conformă cu regulamentul. Autoritățile de protecție a datelor (cum ar fi ANSPDCP în România) au sancționat în ultimii ani mai multe companii tocmai pentru utilizări ale mesageriei care păreau inofensive până în momentul inspecției.

Realitatea operativă actuală este că riscul este scăzut sub aspectul probabilității – se întâmplă foarte rar ca o inspecție a Autorității să auditeze instrumentele de mesagerie specifice ale unui birou de dimensiuni medii – dar ridicat sub aspectul impactului, dacă se materializează. Este un risc pe care majoritatea și-l asumă fără să știe că și-l asumă. Adică, fără a fi evaluat dacă instrumentul utilizat este în concordanță cu responsabilitatea legală a operatorului.

Urma digitală este retroactivă

Există un al doilea argument, aproape simetric cu cel anterior, pe care merită să-l anticipăm: *„dacă aceasta ar fi o problemă serioasă, administrația ar fi început deja să o controleze"*. Realitatea actuală observată îi dă dreptate la suprafață. Controalele pentru utilizarea necorespunzătoare a mesageriei în companiile mici și mai ales la persoanele fizice autorizate sunt astăzi aproape inexistente – nu pentru că comportamentul ar fi permis, ci pentru că administrației din România și din mare parte a UE îi lipsesc resursele umane necesare pentru a audita milioane de entități obligate.

Aceasta este ceea ce sugerează practica observată astăzi. Dar nu este ceea ce sugerează deceniul următor. Doi vectori converg pentru a schimba echilibrul în intervale de timp relativ scurte.

În primul rând: urma digitală este retroactivă. Orice mesaj trimis printr-o aplicație cu server central rămâne înregistrat – cel puțin în metadate – într-o infrastructură care persistă. Ceea ce s-a trimis acum șase luni este tehnic încă audital în prezent. Ceea ce se trimite astăzi va fi audital peste cinci ani. Absența unui control în prezent nu este o garanție a absenței unui control viitor. Este o amânare a evaluării, nu o scutire.

În al doilea rând: capacitatea de audit administrativ va crește accelerat. Introducerea instrumentelor de inteligență artificială în procesele de control elimină blocajul uman care, până acum, a protejat – de fapt, nu de drept – companiile mici și liber profesioniștii. Un sistem capabil să coreleze volume masive de metadate, declarații fiscale, registre comerciale și obligații de notificare a breșelor de securitate nu are nevoie de inspectori: are nevoie de acces. Iar accesul este perfect realizabil prin solicitări adresate furnizorilor cu prezență legală în UE, în cadrul normativ actual.

La aceasta se adaugă un factor mai puțin tehnic, dar la fel de determinant: statele europene se află într-un proces de creștere continuă a îndatorării și trebuie, aproape fără excepție, să-și lărgească baza de impozitare. Sancțiunea administrativă derivată din nerespectarea GDPR este, în termeni pur fiscali, o sursă de venituri în creștere și convenabilă din punct de vedere politic. Nu este o presupunere: este o tendință observabilă în rapoartele anuale ale autorităților europene de protecție a datelor, unde volumul total al sancțiunilor crește de mai mulți ani fiscali consecutivi.

Concluzia operativă pentru operator nu este alarmistă, ci sobră: **decizia privind modul în care este gestionată astăzi comunicarea cu clienții este evaluată în raport cu capacitatea de control a anului în care vine controlul, nu cu cea actuală.** Iar acea capacitate va fi, într-un termen rezonabil, substanțial diferită de cea de astăzi. Cine începe să facă lucrurile corect de astăzi nu va fi în regulă doar de azi înainte: urma generată din acest moment va fi conformă cu norma, iar acest lucru protejează retroactiv perioada următoare. Cine continuă ca până acum va acumula o urmă auditală a cărei conformitate va fi evaluată conform standardelor – și resurselor – anilor care vor veni.

Ce se schimbă cu o altă arhitectură

Există alternative tehnice în care datele nu sunt stocate în infrastructura unor terțe părți, ci călătoresc direct de la dispozitivul expeditorului la cel al destinatarului. În această arhitectură, conformitatea cu GDPR în ceea ce privește transferurile internaționale nu depinde de clauzele contractuale standard, nici de bunăvoința furnizorului, nici de auditurile viitoare. Depinde de faptul că *nu există un transfer*. Iar ceea ce nu există nu poate fi încălcat.

Aceasta nu este o soluție exclusivă și nici singura posibilă. Dar este structural diferită, iar conformitatea normativă încetează să mai fie o anexă procedurală și devine o consecință directă a designului. Pentru un profesionist care își ia în serios responsabilitatea de operator, acea diferență contează.

Următoarea ediție a Cuadernos va analiza în detaliu hotărârea Schrems II și implicațiile sale practice pentru companiile mici și mijlocii dependente de serviciile cloud din SUA, la cinci ani de la publicarea sa.

Surse și cadru normativ

- Regulamentul (UE) 2016/679 (GDPR), în special capitolul V privind transferurile internaționale.
- CJUE C-311/18 („Schrems II”), 16 iulie 2020.
- EDPB – Recomandările 01/2020 privind măsurile care completează instrumentele de transfer.
- Autoritățile de protecție a datelor (inclusiv ANSPDCP) – Rapoarte anuale cu cazuistică de sancțiuni pentru utilizarea necorespunzătoare a mesageriei instantanee în medii profesionale.

← PrecedentSecretul profesional în era digitalăUrmător →Când nu este nimeni la mijloc

Lecturi recente

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Luaţi acest articol cu dumneavoastră oriunde aveţi nevoie.

↓ Markdown ↓ Text simplu ↓ PDF

Fișierul se va descărca pe dispozitivul dumneavoastră. De acolo îl puteți salva, importa în Solo2 sau partaja oriunde doriți. Cuadernos nu decide destinația în locul dumneavoastră.

Sigiliu de ceară · SHA-256 42f97e58918cb015bb2828489588225573dd4f10315575e21e66593a482918d2

Cuadernos Lacre · O publicație a Menzuri Gestión S.L. ·
scrisă de R.Eugenio · editată de echipa Solo2.