Analysis · May 16, 2026

← Previous·Next →

GDPR and Professional Messaging: Why Most Are Non-Compliant Without Knowing It

Almost any firm, clinic, or consultancy sends documents with client data through applications whose server is outside the European Economic Area. Without bad faith, but in many cases violating the regulation without anyone having warned them.

The Document That Travels More Than You Think

A daily situation: a tax advisor receives a document with a client's data via messaging. A salesperson forwards a quote to a colleague via chat. A doctor shares a clinical report with a colleague the same way. No one thinks twice about it. It's normal. It's convenient. It's what is done in any office in any city in Europe every day.

But that document, in many cases, has just traveled to a server in the United States. It has been stored—even if temporarily, even if "encrypted at rest"—in a cloud that neither the professional nor their client controls. It has passed through systems that can technically index metadata associated with the content. And the European General Data Protection Regulation has something quite clear to say about that.

What the Regulation Requires

The GDPR—and by extension the jurisprudence of the Court of Justice of the European Union (in particular the Schrems II ruling, C-311/18, of 2020)—establishes that the personal data of European citizens must be adequately protected. If that data leaves the European Economic Area, the controller must ensure that the recipient offers a level of protection "essentially equivalent" to the European one. In practice, this means that sending client data through services whose servers are under US jurisdiction, without having performed an impact assessment and having implemented supplementary safeguards—standard contractual clauses, additional technical measures such as verifiable encryption, etc.—can constitute a violation of the regulation. Even if no one has said anything yet.

And it is not just about the content of the messages. Metadata—who sends what to whom, when, with what frequency, from where—is also personal data according to the regulations, according to repeated interpretation of the European Data Protection Board. A service that collects metadata of a user's professional communications is processing personal data of that user's clients, without them having knowledge of it, nor having provided any consent for such processing.

The common mental framework—"I only use the app to write; the app is not a data provider for my client"—is legally incorrect. If the client's data passes through a third party's infrastructure, that third party is processing that data. And if it is processing it, there must be a legal basis, a data processing agreement, and appropriate guarantees.

Who Is Responsible

The question of who bears legal responsibility is not academic. The GDPR distinguishes between the *controller* (who decides what data is processed and for what) and the *processor* (who does it materially, on behalf of the controller). The professional who sends client documents is the controller. The messaging app provider is, in many cases, a de facto processor. Without a processing agreement—and without most of the clauses that such a contract should contain—the controller has not fulfilled their obligation.

The benign interpretation is: "most professionals do not know this." The rigorous interpretation is: "ignorance does not exempt from compliance." And the interpretation of any data protection lawyer consulted in this regard is, generally, the rigorous one.

For Whom This Matters Specifically

For any professional or company that handles, even occasionally, personal information of third parties:

- Lawyers who receive client documentation (contracts, lawsuits, statements, asset reports).
- Doctors and other health professionals who share health data—considered a *special category* by Art. 9 GDPR, with a reinforced regime.
- Tax advisors and administrative managers who move identifying, fiscal, and banking data.
- Human resources departments that manage labor and personal documentation of employees.
- Salespeople who receive contact data and, often, sensitive commercial information from prospects and clients.

In all cases, the information is protected by the GDPR. In all cases, in common practice, that information transits through channels whose jurisdiction does not allow being declared "essentially equivalent" to the European framework without additional safeguards. Not out of bad faith. Out of habit. And because of a technological infrastructure that has prioritized convenience over compliance for fifteen years.

The "Everyone Does It" Argument

It is worth anticipating the most frequent objection: "if everyone does it, it cannot be a real problem." It is a perfectly understandable argument and, legally, it has no force. The fact that a practice is widespread does not make it compliant with the regulation. Data protection agencies have sanctioned several companies in recent years precisely for messaging uses that seemed harmless until the moment of inspection.

Current operational reality is that the risk is low in terms of probability—it is very uncommon for an inspection to audit the specific messaging tools of a medium-sized firm—but high in terms of impact if it materializes. It is a risk that most assume without knowing they are assuming it. That is, without having evaluated whether the tool used is aligned with the controller's legal responsibility.

The Digital Trail Is Retroactive

There is a second argument, almost symmetrical to the previous one, worth anticipating: *"if this were a serious problem, the administration would have already started inspecting it"*. Current operational reality gives it superficial merit. Inspections for improper messaging use in small companies and, above all, in self-employed individuals are almost non-existent today—not because the behavior is allowed, but because the administration lacks the necessary human personnel to audit millions of obligated parties.

That is what observed practice suggests today. It is not what the next decade suggests. Two vectors converge to alter the balance in relatively short terms.

First: the digital trail is retroactive. Every message sent by an application with a central server is recorded—at least in metadata—in an infrastructure that persists. What was sent six months ago is still technically auditable

today. What is sent today will remain auditable in five years. The absence of present inspection is not a guarantee of absence of future inspection. It is a postponement of evaluation, not an exemption.

Second: administrative audit capacity will grow rapidly. The introduction of artificial intelligence tools in inspection processes eliminates the human bottleneck that has so far protected small companies and the self-employed. A system capable of crossing massive metadata, tax returns, commercial registries, and breach notification obligations does not require inspectors: it requires access. And access, through requirements to providers with legal presence in the EU, is perfectly feasible under the current regulatory framework.

Added to this is a less technical but equally decisive factor: European states are in a sustained process of increasing debt and need, almost without exception, to expand their tax base. The administrative sanction derived from GDPR non-compliance is, in purely fiscal terms, a growing and politically convenient source of income. It is not conjecture: it is an observable trend in the annual reports of European data protection agencies, where the total volume of sanctions has been rising for several consecutive years.

The operational conclusion for the controller is not alarmist, but cold: **the decision on how client communication is managed today is evaluated against the inspection capacity of the year the inspection arrives, not against the current one.** And that capacity will be, in reasonable terms, substantially different from today's. Whoever starts doing things right today will not only be in compliance from today: the trail generated from this moment will be consistent with the regulations, and that retroactively protects the coming segment. Whoever continues as before will be accumulating an auditable trail whose conformity will be evaluated against the standards—and resources—of the coming years.

What Changes with a Different Architecture

There are technical alternatives in which data is not stored in third-party infrastructure but travels directly from the sender's device to the receiver's. In that architecture, GDPR compliance regarding international transfers does not depend on standard contractual clauses, nor on the provider's goodwill, nor on future audits. It depends on the fact that *there is no transfer*. And what does not exist cannot be non-compliant.

This is not an exclusive solution nor the only one possible. But it is structurally different, and regulatory compliance ceases to be a procedural annex to become a direct consequence of design. For a professional who takes their responsibility as a controller seriously, that difference matters.

The next issue of Cuadernos will analyze in detail the Schrems II ruling and its practical implications for small and medium-sized enterprises that rely on US cloud services, five years after its publication.

Sources and Regulatory Framework

- EU Regulation 2016/679 (GDPR), especially Chapter V on international transfers.
- CJEU C-311/18 ("Schrems II"), July 16, 2020.
- EDPB — Recommendations 01/2020 on measures that supplement transfer tools.
- Annual reports from data protection agencies with case studies of sanctions for improper use of instant messaging in professional environments.

← PreviousProfessional Secrecy in the Digital EraNext →When no one is in between

Recent readings

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Take this article wherever you need it.

↓ Markdown ↓ Plain text ↓ PDF

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 ee90b4f9a71dcce5e8216298a6a8f66dfd72b043c1073d83d79df6b10cb26a3d

Cuadernos Lacre · A publication of Menzuri Gestión S.L. ·
written by R.Eugenio · edited by the team of Solo2.