Reflection · May 16, 2026

← Previous·Next →

Professional Secrecy in the Digital Era

When communication between the professional and their client passes through a technically inadequate channel, secrecy is not broken on the day of the leak. It was broken much earlier, at the moment the tool was chosen.

A Problem Almost No One Sees

A lawyer receives a sensitive document from a client on their phone. A doctor discusses a delicate diagnosis with a colleague. A psychologist coordinates a patient's treatment with a psychiatrist. A tax advisor sends data for a pending return review. All do so through instant messaging. And almost none stop to think where those messages actually end up.

The answer, in most cases, is the same: in a server the professional does not control, in a country whose legislation they do not necessarily know, managed by a company whose business model is—in direct economic terms—to accumulate data. The message may be encrypted in transit. But once it reaches the server, it is a stored copy in a third party's infrastructure, subject to that third party's operational, legal, and commercial decisions. Not the professional's.

What Legislation Says

The European General Data Protection Regulation is unequivocal in its Article 32: whoever processes personal data must apply "appropriate" technical and organizational measures to ensure a level of security appropriate to the risk. The adequacy of measures is not evaluated against "what the app says it does," but against the real risk. If a client's data ends up on a server whose jurisdiction does not guarantee a level of protection equivalent to that of the European Economic Area, the controller—that is, the professional—is assuming a risk they are probably not fully aware of.

And it's not just the GDPR. Professional secrecy, specifically regulated for lawyers, doctors, psychologists, auditors, journalists, and others, requires that communication with the client be confidential. Not "confidencial to the extent possible." Confidential without qualifiers. If the technical channel used cannot guarantee it, the professional is assuming a risk that their profession's ethics do not allow.

The paradox is that the risk is invisible. No one audits the law firm's messaging. No one asks for the data processing contract from the chat provider. The risk emerges only when it's too late: a leak, a published breach, a court order fulfilled on another continent without user notification.

What a Professional Technically Needs

What a professional bound by professional secrecy needs is, in reality, surprisingly simple from a requirements standpoint:

- A channel where messages go directly from the sender's device to the receiver's, without passing through an intermediate server that stores copies.

- An infrastructure whose jurisdiction and policies are aligned with the GDPR by construction, not by declaration.
- A way to identify oneself to the interlocutor without having to hand over professional contacts to a third party (client names, phone numbers, address book).
- Some verifiable system—not based on the provider's word—to confirm that the message reached the correct person.

It is not a demanding list. It is, in fact, what was taken for granted in pre-digital professional communication. A certified letter met all those criteria. A telephone call from the firm's switchboard to the client's also did. What is strange is not that these guarantees are requested today: what is strange is that they have been lost when moving to the digital channel, without anyone noticing.

The Difference Between Encrypting and Not Storing

There is a useful metaphor. Encrypting a message and storing it on a server is equivalent to putting a document in a safe and leaving the safe in a stranger's house. The safe is good. The document, in principle, cannot be read. But the document *remains in someone else's house*. And that someone else can receive a court order, can suffer a cyberattack, can change their terms of service, can be bought by another company with different ethics, can disappear tomorrow.

The structural alternative—not procedural, not based on trust—is for the document to never leave the office. That it travels directly from the professional's desk to the client's desk, without passing through any intermediary. That is what point-to-point communication between devices technically does: it eliminates the intermediary. It's not that the intermediary is bad. It's that, for the case of professional secrecy, the intermediary is *unnecessary*. And the unnecessary, in any system aspiring to be secure, must be eliminated by principle.

The Question of Responsibility

In the end, the question that every professional with a duty of secrecy should be able to answer with a resounding yes is the following:

> If tomorrow a conversation with one of my clients is leaked and a court or a professional association asks me how I manage confidentiality, can I technically demonstrate that the channel I used does not store copies on third-party infrastructure? Can I prove that the data never left the devices of the two people who participated in the conversation? Can I demonstrate, without depending on the word of a company from another continent, that confidentiality was guaranteed by architecture and not by a promise?

If the answer is no, the problem is not the specific tool. The problem is that responsibility has been delegated to a tool that was not designed to support it. It's like putting confidential files in a transparent envelope and trusting the mailman won't look.

The tool a professional chooses to communicate with their clients says a lot about how they value their trust. There are tools designed so that trust does not depend on promises, but on architecture. And there are tools that are not. Knowing the difference is part of the job.

Cited Regulatory Framework

- EU Regulation 2016/679 (GDPR), especially arts. 5, 25 (data protection by design) and 32 (security of processing).
- Organic Law 6/1985 on the Judiciary and professional statutes regarding the duty of professional secrecy.
- Law 41/2002 regulating patient autonomy, art. 7 (confidentiality of health information).
- Deontological Codes of professional associations regarding confidentiality and professional secrecy.

← PreviousEncryption Is Not Privacy: What Metadata Tells About YouNext →GDPR and Professional Messaging: Why Most Are Non-Compliant Without Knowing It

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 af066613942809ffaef1cf9cbdfa2937238a4228136577f76511c1efb9069989

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