Reflection · May 26, 2026

← Previous

What a signature cannot fix

When a technical channel is not suitable for sensitive data, no signed authorization makes it adequate. The only thing a signature changes is the false peace of mind of whoever collects it; the data follows exactly the same path.

To be clear: In the meeting someone says it with the best intention: «everyone uses WhatsApp; just have the clients sign an authorization and that's it». It sounds like diligence — there is a piece of paper, a signature, a date. But that signature does not move the data, and the person who signs it is almost never the only person whose privacy travels through that channel. And even if they were, no signature legalizes an illegality.

The way out that seems like common sense

The scene repeats itself in offices, clinics, and consultancies — and also in much less solemn places. The painter who sends photos of a client's apartment. The plumber who forwards an invoice with the name, address, and phone number. The taxi driver who saves in his phone the address of whoever he picks up every morning. The freelancer who sends by chat the ID of whoever hired him. It doesn't take a legal movie case for data of people other than oneself to circulate on a phone.

And in any of those places, sooner or later, the same elegant way out appears. Someone raises the doubt — is it right to send this through here? — and, before the conversation gets uncomfortable, the comfortable answer arrives: just have the client sign an authorization. If they give permission, it's done.

It is an attractive way out because it resolves the discomfort without forcing a change of tool, without learning anything new, without cost. It has the shape of diligence: a document, a signature, a date. And yet, it does not solve the problem it intended to solve. It covers it up.

A signature does not move the data

It's best to start with the simplest, because it is exactly what gets overlooked. An authorization is a piece of paper. It does not change where the message travels, nor on what server a copy remains, nor who can read it if the appropriate order arrives or if there is a breach. The client's document will continue passing through the same infrastructure, in the same country, managed by the same company, with or without the signature.

The only thing that changes with the signature is the professional's state of mind: they go from doubt to a false peace of mind that does not correspond to any real change in the data's journey. The signature is a permission one grants oneself to keep doing exactly the same thing.

The permission no one in the room could give

Here lies the edge of the matter. Think of a divorce. The client signs the authorization: fine, let their data go wherever necessary. But it's not just the client's data traveling through that channel. The other party's name

travels. The data of the minor whose custody is disputed travels. The expert's report, a third party's testimony, the spouse's account number travel.

None of those people have sat in the office. None have signed anything. The professional has obtained permission from the only person who wasn't the whole problem, and has continued processing the data of all those who were without asking them anything — because they couldn't.

The same goes for an employment record mentioning other employees, a medical report mentioning relatives, a statement gathering the client's own providers and clients. A third party's information does not stop being protected because the person providing it signed a piece of paper. It was not theirs to authorize.

There are things a signature cannot reach

There is a limit we almost never test: a signature only goes as far as what is yours. What is yours you can give away. Someone else's, no — no matter how well you sign your name.

A parent cannot sign a permission for their child to be harmed. That piece of paper is worthless, and not because it lacks a stamp: because that permission was never theirs to give. The client's authorization works the same way — it covers theirs and stops there.

And not even within that limit does it cover everything. A signature does not make lawful what the law does not consent to, no matter who signs it. Consent is not a master key: it is a key that opens only one door —one's own —, and not even that door leads to what is prohibited.

And it must be said bluntly, because it is the part that is almost never said: asking for —or giving— a signature to shield what the law does not allow is not a neutral gesture that simply has no effect. Depending on the case, attempting it is, by itself, a new infringement. It does not fix the problem: it makes it worse.

The signature that backfires

And there is a twist that should be faced head-on. Collecting the authorization does not leave the professional as they were: it leaves them worse off.

Because that piece of paper is, first and foremost, the proof that someone asked the right question — is this appropriate? — and answered it with a placebo instead of a solution. The day it is necessary to explain why a third party's data ended up where it shouldn't have, the signed authorization will not be the shield imagined: it will be the document proving the risk was known and the choice was made to cover it with a signature. Apparent diligence leaves a trace. The signature does not archive the problem; it dates it.

The only thing that does fix it

If a signature fixes nothing, what does fix it? Only one thing: that the data does not go where it shouldn't go.

When the channel does not deliver a copy of the document to a third party — because it goes directly from the sender's device to the receiver's device, without a server in the middle storing it — there is nothing to authorize, no one to ask for permission, and no uncomfortable trace to justify later. The problem is not managed with a form: it disappears because the architecture doesn't even create it.

This is not a property of a single tool — it is a property of design, and there is more than one way to have it. What distinguishes these tools from the rest is not a better-written promise in the legal notice, but that they do not need anyone to sign to be compliant.

A signature is the civilized way of asking permission. But you can only ask permission from someone who is in front of you. And in almost every piece of sensitive data a professional handles, the people whose privacy is truly at stake are not in the room, they are not going to sign, and they would have no reason to trust someone to sign for them. That is why the right question was never «how do I get this authorized?», but «why do I need authorization for something a well-chosen channel wouldn't force me to ask for?».

Editor's note: when these Cuadernos name companies or products, it is not to accuse. Those who build them do work that millions of people use and appreciate. What we point out is structural — the model, not the brand. Brands appear as examples because they are the ones the reader recognizes.

Further reading

- This Cuaderno purposely leaves aside the regulatory detail —the articles and the rulings—, because the argument it dismantles is not legal: it is a comfortable way out. The legal framework of why the channel matters lives in the next two Cuadernos.
- *GDPR and professional messaging: why the majority fails to comply without knowing it* — international transfers, data controller, and retroactive digital footprint.
- *Professional secrecy in the digital age* — why confidentiality must be guaranteed by architecture and not by promise.

← PreviousReal vs. apparent privacy: the questions to ask yourself

Recent readings

- Analysis · May 26, 2026 Real vs. apparent privacy: the questions to ask yourself
- Analysis · May 25, 2026 Self-hosting as a professional practice
- Concept · May 23, 2026 The 24 words: what a cryptographic identity is

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 272b4805750fe6697a111a7e67cc1570ac4f2e4f7f528df21bcb596ec107c500

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