Analysis · May 25, 2026

← Previous·Next →

Self-hosting as a professional practice

A server is nothing more than a computer. The question is not whether one should have one, but where the data of your clients lives, who maintains it and who assumes the responsibility when something fails.

To understand each other: Your data lives always in someone's computer: in that of a giant whom you trust everything, in a rented one that you manage, or in your own. More control you want, more responsibility you assume. Delegating in a large third party reassures, but doesn't exempt: the information is yours —and that of your clients—, and the responsible person is you.

The question between the cloud and the basement

It is good to start by deactivating a word that scares without reason: server. A server is not a mysterious machine in a cooled room. It is, simply, the computer of another person —or your own— that saves information and delivers it to whoever requests it. For decades we kept the information of our clients in a folder, in a filing cabinet, on the office desk and no one lost sleep for that. Information was not scary because it was on paper; it doesn't have to be scary either because it is on a disk.

The «cloud» is not ethereal either. It is the computer of a company, almost always far away and almost always someone else's. I learned this involuntarily the day that, confident that my files were in safe custody in Google Drive, I discovered that the folder on my computer did not contain my documents, but shortcuts to documents that lived somewhere else. If that other place decided to close, change the price or cancel the service, my tranquility would go with it. I did not possess my things; I had permission to access them.

That is where the question of this Notebook arises, easier to state than to answer: where should your clients' data live? And your own? The public conversation frames it as if there were only two opposing answers — the cloud of the big platforms, or doing it yourself — almost a matter of which side you're on. But there aren't two paths: there are three, and none of them is an act of faith. Read slowly, they have more nuance and ask more of you than they seem to.

This concerns you, whatever you sell

It is easy to think that confidentiality is a matter of lawyers, doctors or journalists, and that the rest have nothing to hide. It is a error, and of the expensive ones. Almost any business keeps data of its clients subject to the law, and many keep, without knowing it, information quite more sensitive than it seems.

A sofa shop writes down the name, address and phone number of whoever buys; if there is financing, their financial details too. A renovation or interior-design firm keeps photos of the inside of its clients' homes and the full floor plans of their houses. A cleaning company handles the floor plans of the offices it cleans, often marked with colours and numbers that say which employee goes where, at what time and with which key. None of that seems like much until you ask who else it would be valuable to: those cleaning plans are, seen through other eyes, the perfect map for anyone who wants to break in and steal.

The fact of a business being small, or that it sells sofas instead of defending pleas, doesn't make its data lack of value nor makes the law stop applying to it. It only makes its owner tend to think less in it. And thinking little about something that is your responsibility is precisely where problems begin.

Where does your data live?

There are, in essence, three answers to that question. And it is worth remembering that “the data” is not only a client's dossier or the stack of invoices and quotes: it is also your conversations with them — over WhatsApp, over a professional chat service, over Solo2. The three answers that follow are not degrees of purity nor a ladder from good to bad: they are three ways of distributing the same thing, control and responsibility.

Delegate everything to a provider. It is the most common approach, and for most people it is the only one they know. I put everything in Google Workspace or Microsoft 365 and entrust it entirely to the provider. I pay my fee and stop thinking about it. The most extreme form of this is the services where you don't even get to hold your own data: certain cloud billing programs, for example, keep your invoices and quotes — and work very well — but the information lives in their system, not yours. As long as you pay, you have access; the day you leave, you discover that taking your own history with you is hard or impossible. Holding your data half-hostage is, for more than one provider, exactly what stops you from leaving for a competitor. In exchange for convenience I hand over control and — without saying it out loud — the feeling that the responsibility is no longer mine. Here a nuance fits that almost never gets made: delegating is not a synonym for American. I can delegate everything just as comfortably to a European provider — Infomaniak, for example — and resolve at a stroke much of the doubt about international transfers that we saw in “Schrems II”, without self-hosting anything. It is not the United States against the rest of the universe: within pure delegation there are already decisions that matter.

Renting and managing your own server. I have the same thing that Microsoft or Google would give me, but I set it up myself. I rent a server at a European provider —Hetzner, OVH, Scaleway—, install free software (Nextcloud for files, for example) and manage the result myself. I gain real control: I know what is running, where and why. But the machine is still in the data center of a third party and above all, who bears the consequences changes. By delegating, if something fails, you have someone to blame. By managing it yourself, the most likely is that the fault is yours.

Having it on your own computer. This is the option that almost no one tells about, and it is the heart of this Notebook. You don't need an enormous server turned on twenty-four hours a day inside a macro data center to host your things. Your office computer is already a server: it serves you. You leave it on at the office and you connect to it from the laptop at a client's house, or from the mobile when you are at home. We call it «the office computer», not «the server», but it does exactly the same thing as the two previous options. The control is maximum and so is the proximity: your data is where you are. The flip side, said without frills, is that the responsibility is also maximum. If the power goes out there is no technician on duty in Nuremberg: it is up to you to lift the breaker. And so that that computer is accessible from outside, something is needed that throws the bridge between your laptop and it. It is not magic, and it is good to know it before choosing this path.

And you don't even need to repurpose the office computer: there's a device designed for exactly this, the NAS (made by Synology, QNAP and others). Like almost everything we've seen in these Cuadernos, there's no magic inside: it's a specialized computer, the same kind of machine you'd rent in a data center, only built to store data and serve it over the network, with no monitor or keyboard in between. Plug a screen and a keyboard into it and you have an ordinary computer; install the right software on your PC and you have a NAS. The difference is that the NAS comes ready to use. You buy it, you plug it in at home or at the office, and it's yours. You don't pay a monthly fee; you pay once and it belongs to you, like any other tool of your business. You turn it on, turn it off, take it somewhere else if you wish. And since it's yours, nothing stops you from having two —one at home, one at the office— or three, adding one in a secure location, synced with each other: your own redundancy, without depending on a third party to maintain it. Self-hosting, in the end, isn't a single thing: it's a combination of machines, of ownership, of locations and of software.

Here it is unavoidable to name what we do, and we do so without disguise: in Solo2 that bridge is built by the application itself. The computer in your office stays accessible only to your trusted devices, and always under encryption, and your other devices reconnect to it on their own. When a client talks to you, it is your computer — not a third party's — that talks to the client. We don't solve the power cut; we solve the bridge. And we are not the only ones: for almost every need there are programs today — free or proprietary — that allow exactly this, keeping the data on your own machine and reaching it from outside. Ours is an example; what matters is the idea, not the brand.

Redundancy is not a superpower

Here arises the immediate objection, and it is reasonable: if I have everything on the office computer, what happens if it breaks? The question is good. The answer is that the safety net we imagine in the large providers is more modest —and easier to be imitated— than it seems.

When I leave my data in the data center of a multinational, I trust that it has copies in several places. And probably it has them: in a second location, maybe in a third. But that redundancy is not infinite and above all it is not mine: it remains a hard disk of which I am not the owner, managed by someone in whom I place a faith that I almost never verify.

That same net I can weave myself, and with a decisive advantage. My daily service lives on the office computer. From there I keep an encrypted copy on the computer of a friendly company —a colleague in the profession, another trusted office— and another encrypted copy, if I want, at that same European provider we were talking about. The difference is everything: what I leave outside is not my service nor my data in clear, but an encrypted copy that only I can open. The external provider keeps a closed chest of which he doesn't have the key. I do not entrust my information to him: I entrust him some bytes that without me signify nothing.

It was safe until it wasn't anymore

Allow me a personal story, because it illustrates this better than any argument. For more than ten years I was a devoted customer of CrashPlan, a technically extraordinary backup service. I backed up in their cloud all my computers and those of my family —those of the company and those of the house, everything—, with versions that I could recover with the frequency I wanted, traveling back in time to a specific file from months ago. After the first copy it only transmitted the differences, encrypted and compressed, so that I kept an enormous backup updated with almost no effort. It saved me many times, from a silly document to a whole disk. The price went up over the years and I didn't care: I paid happy.

What I didn't know was that CrashPlan had made a calculation error: they had promised by contract unlimited storage, in space and time. And space multiplied by time —years of history, versions every few minutes— grows until it becomes unsustainable. One day they informed us all that the service was ending. They did it with elegance and with a generous term, almost a year, and gave us means to download our own. But where does one go with more than ten years of versioned copies of all their disks? There you discover that you have neither the way to download everything nor the place to put it, and that, even if you could, the new warehouse would cost a fortune.

I saved four essential things. The rest went when they flipped the switch. I was calm, my information was safe... until it stopped being so. And not through betrayal: CrashPlan behaved impeccably — unlike Evernote, which years later behaved shamefully — quite simply, my guardian angel in the cloud decided, fully within its rights, to stop being one. The result, for me, was identical: what I thought was safe vanished.

What this story really teaches has more to do with human nature than with technology. When someone feels that something is their responsibility, they act in a preventive way: they make copies, they secure their back, they distrust with good judgment. When they believe —erroneously— that the responsibility is borne by a large and

solvent third party, they relax and let things go. That delegated tranquility is not prudence: it is, without makeup, a form of irresponsibility.

Paying is not the same as complying

That quiet irresponsibility resembles much that of some parents who enroll their son in the most expensive school, pay him afterwards a master degree, and with that they believe they have fulfilled their duty. They have not fulfilled. Being a parent is worrying about what he learned today, about what he doesn't understand, his values, his self-confidence. If at twenty-five years old that son doesn't know how to work nor behave, the fault is not of the school that collected the money: it is of the one who delegated and paid believing that with that it was enough. Paying a third party does not exempt from responsibility. It never has.

It is the same with data, and recent history confirms it. Fifty or a hundred years ago a professional kept their clients' things in folders, in the office or at home, and felt responsible for them. Rarely was anything lost. We have moved into the digital world and, with astonishing ease, we upload everything to “the cloud” — which is nothing more than some multinational's computer — and stop worrying. And often there are accidents, and there are firms that lose everything, and then people say: it was Google's fault, it was Microsoft's fault. No. The information is yours, or your clients', but the one responsible is you.

Hosting your own things is not a technical whim: it is recovering that serenity of decades ago, that of knowing where each thing is and why. Data protection, meanwhile, has lived an abrupt pendulum swing —from there not being any norm, when anyone exhibited the data of a client without thinking, to a requirement that falls with disproportionate hardness on the smallest, the freelancer who gives the phone of a client to the delivery person. I do not discuss the goal; I observe the mismatch. But the mismatch does not absolve us: the day that the administration has means to track and sanction at scale, size will stop protecting anyone, and it is wise not to wait for that day with the house unordered. Having the data under own control helps to comply and helps to prove it. And above all, it returns things to their place: when information is yours, the responsibility is entirely yours —there is no third party to blame, nor a third party whose failure exposes you—.

Responsibility also protects

It would be dishonest to paint this without its shadows. Taking the intermediary's place means carrying what comes with it: keeping backups up to date, applying updates, and a legal responsibility — that of the RGPD — which, in truth, never quite stopped being yours (the footnote references detail the articles). There is work, and there is a day when something fails at the worst possible time. We don't hide it.

But the fear that surrounds that word, responsibility, is miscalibrated. It is far easier to lose your files in a cloud service that shuts down, or your photos in Google Photos, than to lose that folder of important documents on your own computer: the one you know where it is and would notice missing the moment it disappeared. What you feel is yours, you look after; what you believe to be safe in someone else's hands, you neglect.

Think of the photo albums of old, the ones with developed paper kept in a drawer. Have you ever heard anyone say they “lost” their family album? You hear about the house that burned down with the album inside; losing it just like that, no. And yet, people who had all their photos in Google Photos or Apple Photos and were left with nothing: that story comes back every few months, because they believed it was safe. Google Photos looks after your photos, of course it does; but it does not look after them the way parents look after the album where their children and grandchildren are. That difference is not fixed by any data centre: responsibility, when it is yours, is not only a burden; it is also the best guarantee.

Four questions before deciding

If you are considering taking the step, in any of its forms, it is good to answer first four questions with dispassionate honesty:

1. Which part of your data would it hurt to lose, or to be unable to take with you? And beware of dismissing the “routine”: the invoice history seems the most prosaic thing in the world until you switch programs and discover that those invoices belonged to the provider, not to you — that, at best, you can print them to PDF, with no way left to search inside them. It is not just a matter of sensitivity: it is about who truly owns what you need to keep.
2. Which option is proportional to your real technical ability? A well-kept computer of your own is within anyone's reach; administering a whole server, not so much. Be honest about what you know and what you don't. And remember that between setting up a whole server and delegating everything there is a very reasonable middle ground: programs — free or proprietary — that keep your data on your own machine and let you reach it from outside. For many people it is the best balance.
3. What plan do you have for the worst day? A breach, a dying disk, a provider that closes, the technician on sick leave. If the plan starts with «this shouldn't happen», it is not a plan.
4. Would you know how to prove that you comply if tomorrow you were inspected? Doing it well and being able to prove that you do it well are not the same thing. The law asks for the second.

There is no universal answer. There is a proportionate answer, adopted with honesty about what is gained and what is inherited. And above the technique, a simple certainty: your data lives in someone's computer. The only question that really matters is whose computer you want that to be.

Self-hosting is neither a virtue nor a vice: it is a tool with a concrete footprint of capabilities and responsibilities. The question was never whether to host your own data, but what data, how, and with what support network. Regaining control of data is not returning to the basement nor distrusting everything: it is returning to feeling responsible for what is ours, just as when that data lived in a folder on the desk. That responsibility, correctly understood, is the real service that a professional provides to their clients.

Sources and further reading

- Regulation (EU) 2016/679 — article 28 (processor), article 32 (security of processing), article 33 (notification of a breach), article 37 (designation of the Data Protection Officer).
- Spanish Data Protection Agency — *Practical guide for risk analysis in the processing of personal data* (current revision). Framework for controllers who assume own technical functions.
- European Data Protection Board — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Applicable also for the proportionality test in decisions of own infrastructure.
- European Commission — public directory of information service providers established in European jurisdiction. Administrative starting point to identify European managed hosting options.
- Nextcloud GmbH (Germany) — *Nextcloud Enterprise architecture and compliance documentation*. Documented case of free software with self-hosted and managed by European provider modalities; useful as technical reference of a project maintained in European jurisdiction since 2016.

← PreviousThe 24 words: what a cryptographic identity isNext →Real vs. apparent privacy: the questions to ask yourself

Recent readings

- Reflection · June 29, 2026 You Are Not Anonymous
- Reflection · May 27, 2026 What a signature cannot fix
- Analysis · May 26, 2026 Real vs. apparent privacy: the questions to ask yourself

Take this article wherever you need it.

Wax seal · SHA-256 154d898236fddf69cbc9aed1e9ea3ba94ab3954292bcd3093ab5a9be88c3e170

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