Digital Sovereignty in 2026: From Strategic Vision to Your Daily Reality

Digital Sovereignty in 2026: From Strategic Vision to Your Daily Reality

Bernard Sfez - 2026-05-17 19:18

Since our first update in February, the shift toward European digital sovereignty has accelerated faster than in the previous five years. While EU powers are migrating millions of workstations to Linux and Brussels targets opaque recommendation algorithms, the push for sovereign tools is no longer a theory—it is a massive public sector transition to assume European digital sovereignty. Yet, as governments pivot, data vulnerabilities are peaking: three accounts are compromised every second, and major national hacks are exposing tens of millions, making Europe a primary target for global cyber-threats. Governments are moving, which is progress. But where does that leave those without a ministerial budget?

This fourth article explores the rapid evolution of the European regulatory landscape during the past four months and maps out the escalating threats of 2026. Most importantly, it provides a concrete action checklist—categorized by time and effort—designed for professionals who need to protect their data and their clients' trust without a dedicated IT department. These are simple, scalable measures you can implement right now, within your means and at your own scale.

In our previous installments, we mapped the scale of our digital dependency, analyzed governmental efforts—and inconsistencies—in addressing it, and established the foundations for a sovereign infrastructure.

This fourth chapter shifts the focus to the practical. We are moving from high-level strategy to daily action for individuals, SMEs, NGOs, local authorities, and freelancers. The mission is clear: ensure data protection (strategy and requirements) and digital sovereignty over your data and your clients' data, secure business continuity, and comply with an increasingly demanding regulatory landscape.

The mission is clear: enforce data protection strategy, improve cyber resilience and digital sovereignty over your and your clients information, securing your business continuity, and ensuring compliance with a regulatory landscape that now applies to every professional.

However, a brief landscape update is necessary. Since our journey began in February, the environment has evolved rapidly—for better and for worse. On the positive side, we have seen landmark legislation, unprecedented migrations to Open Source infrastructure, and a decisive political shift toward autonomy. On the negative side, we face a surge in massive data breaches

and a new generation of AI capable of uncovering thousands of security vulnerabilities in a matter of hours. This technology, which will eventually be our shield, is currently being weaponized to automate sophisticated attacks.

Against this backdrop, we address the question that has become unavoidable for those who lack a ministerial budget or a multinational’s resources: What is our concrete roadmap for action?

The Four-Month Shift: From Strategy to Execution

European Governments Transition to Action

On April 8, 2026, a landmark inter-ministerial summit brought together public operators and private stakeholders with a single mandate: systematically reducing extra-European digital dependencies. While the rhetoric of "Digital Sovereignty" has been around for years, this summit marked a turning point. For the first time, these strategic goals are backed by binding timelines and mandatory transition frameworks.

The shift to European or Open Source alternatives is visible across the continent’s largest public infrastructures:

- The OS Migration: Leading the charge, major French administrative bodies are phasing out Windows in favor of Linux.
- Sovereign Tooling at Scale: The National Health Insurance Fund is currently migrating 80,000 agents to a "Sovereign-First" suite: Tchap for encrypted messaging, France Transfert for secure file sharing, and dedicated internal video-conferencing.
- The Cloud Sovereignty Challenges: Health data platforms, previously hosted on Microsoft Azure, are mandated to transition to sovereign European cloud providers by the end of 2026.
- Mandatory Roadmaps: By autumn, every major department must submit a transition roadmap covering eight critical IT pillars. Workstations, Collaboration Tools, Cybersecurity (Antivirus), AI, Databases, Cloud Infrastructure, Virtualization, and Network Equipment.

This is a pan-European movement—a broader shift toward strategic autonomy.
In Germany, the state of Schleswig-Holstein has already successfully migrated 80% of its 30,000 workstations to Open Source, reporting a direct saving of €15 million in licensing fees in 2026 alone. Meanwhile, the long-standing GendBuntu project (the French Gendarmerie's Linux distribution) now powers over 103,000 workstations, reducing the Total Cost of Ownership (TCO) by an estimated 40%.

Why "This Time" is Different ? Skeptics often point to the "Munich Case" of the early 2000s, where the city famously migrated to Linux only to return to Microsoft years later under intense lobbying pressure. However, the 2026 landscape is fundamentally different. Tensions between the EU and the US have made digital dependency a top-tier national security risk and the Cloud Act and FISA are no longer niche legal concerns; they are now primary drivers of Senate-level debates and corporate risk assessments. We are no longer seeing isolated cities move. With entire countries and European regions pivoting simultaneously, a robust ecosystem of European service providers is finally reaching maturity.

Europe Sets the Global Standard

In February 2026, the European Commission signaled a historic shift in digital sovereignty oversight. By issuing a preliminary finding against TikTok under the Digital Services Act (DSA), the EU has, for the first time, legally targeted the mechanics of recommendation algorithms and their addictive nature. This move marks the transition from regulating "what" is posted to regulating "how" AI amplifies content. This could lead to the end of algorithmic impunity.

A significant legislative precedent is emerging from France that is likely to echo across the EU: Editorial Liability for Algorithms. Under 2026 regulations, service providers can now be held legally responsible for the outputs of their recommendation engines. If an AI massively amplifies disinformation or harassment, the provider is no longer viewed as a passive host but as an Editor-in-Chief. For businesses, this shifts AI safety from a "nice-to-have" to a core legal requirement.

At the same time the regulatory pressure extends to infrastructure and market competition:

- NIS2 Directive: This is no longer just for "Critical Infrastructure." NIS2 now mandates rigorous cybersecurity standards for a vastly expanded scope, including SMEs and local authorities. Compliance is now a prerequisite for participating in the European supply chain.
- Digital Markets Act (DMA): The push for Interoperability is finally dismantling "Walled Gardens." The DMA is forcing major platforms to open their ecosystems, allowing users to interact across different applications. This is a massive opportunity for European challengers to compete with established Big Tech incumbents on a level playing field.

Data Breaches: A Continental Crisis

While institutions legislate, data is hemorrhaging at an alarming rate. France has become a cautionary tale for the rest of Europe: in Q1 2026, it ranked as the second most targeted country in the world, with 23.5 million compromised accounts—a 108% increase over the previous quarter.

The breach of the ANTS (the agency managing national IDs and passports) in April 2026 exposed the data of 19 million citizens. The cause? A Basic IDOR (Insecure Direct Object Reference) vulnerability—a fundamental programming error that allows unauthorized access simply by changing a digit in a URL. This level of failure in a state-level portal underscores a critical business reality: internal oversight is no longer sufficient. Without regular, independent, and third-party security architecture audits, even the most sensitive national databases remain "low-hanging fruit" for hackers.

The contagion is global. Recent international breaches have compromised:

- Financial Infrastructure: The Bulgarian National Revenue Agency saw the tax and social security data of 5 million citizens leaked. In July 2025, TransUnion exposed the sensitive credit data of 4.4 million global customers.
- Healthcare Systems: The Change Healthcare attack (2025/2026) remains the largest in history, with 192.7 million patient records stolen. Aflac recently confirmed a breach impacting 22.6 million individuals worldwide.
- Enterprise Supply Chains: Jaguar Land Rover faced a £1.9 billion loss in late 2025 after a cyberattack paralyzed its UK production plants for weeks. The luxury giant Kering (Gucci, Balenciaga) saw 7.4 million customer records exposed through a compromised CRM system.

For large corporations, a breach is a PR crisis; for an SME, it is often terminal. A Hiscox study found that one-fifth of firms across Europe and the US are in danger of bankruptcy following a major cyberattack. According to Mastercard, 1 in 4 European SMEs believe a single successful attack would force them to close permanently. With the average recovery from a ransomware attack now exceeding three weeks, any small structure without a massive cash reserve faces a literal death sentence.

The most dangerous evolution is not the individual leak, but the AI-powered cross-referencing of data.
Separately, a leaked Social Security number or a bank detail is a risk. Combined, they are a weapon. New AI tools can now ingest millions of disparate records from different breaches to "stitch together" comprehensive identity profiles in hours. This automation of identity theft makes every previous leak exponentially more dangerous today than it was six months.

Where does that leave you?

> *The regulatory landscape is shifting. Large institutions are moving. Government ministries have their roadmaps and multi-million euro budgets. Multinationals have CIOs, SOCs, and top-tier consulting firms at their disposal. Meanwhile, data breaches continue to strike everyone indiscriminately.*
>
> *So, where does that leave you? Whether you are an SME, a non-profit, a local municipality, or a freelancer—with or without a dedicated IT department, and with or without a massive*

> *budget—what is your next move, how to improve your cyber resilience?*

The good news is that you don’t need to be an expert to get started. You don’t need to do everything at once, nor do you have to do it alone. Most of the actions outlined below are accessible, progressive, and often free. Some take an hour. Others require a weekend. A few will need a structured plan and perhaps an outside perspective to avoid false starts. This is also an opportunity to start empowering your team and making them feel responsible for these issues. If you lack the time or the process feels too disruptive for your business, specialized providers can develop a reasonable plan tailored to your scale—this is actually a major part of what we do. But the most important thing is to start, because when it comes to data protection strategy, time is already running out.

We have organized the following into a checklist, much like a shopping list. You don’t have to grab everything in one go. Browse the aisles, identify what fits your situation, and start with what feels most urgent or simplest. The rest will follow in time, as long as you stay informed and occasionally read articles like the one you are reading now.

Things that take about an hour (and cost nothing)

Check your passwords

Head over to Have I Been Pwned and enter the email addresses you use on a daily basis.
You will likely discover that several of your addresses already appear in data leaks. If that is the case, change the affected passwords immediately. And if you are using the same password for multiple services, now is the time to stop. A single compromised account opens the door to all the others.

Can you trust this site?
Have I Been Pwned was created in 2013 by Troy Hunt, a renowned Australian security expert who has notably testified before the US Congress regarding data breaches. The service has been fully open source since 2021, and its code is verifiable on GitHub. The governments of Australia, the United Kingdom, and Spain officially use it to monitor their domains. The FBI directly feeds compromised credentials discovered during its investigations into the database. You only enter an email address, never a password. In the interest of total transparency, it should be noted that Troy Hunt himself was the victim of a phishing attack in March 2025—proof that no one is infallible—but he published the incident on his own platform, which speaks volumes about his integrity.

Install a password manager

KeePassXC is open source, free, and stores your passwords locally on your machine—nothing leaves your premises. Bitwarden is an Open Source alternative if you need to synchronize across multiple devices. It is self-hostable ("in-house"), and this is the kind of setup that a provider like OpenSource Solutions can install and configure for you. Proprietary solutions like 1Password offer undeniably smoother browser and mobile integration. However, you must ask yourself: where are your passwords stored? With 1Password, the answer is on American servers, with AWS, subject to the Cloud Act. In other words, the keys to all your accounts are hosted in the exact jurisdiction this article invites you to move away from. This is a choice to be made knowingly, not a detail. In

any case, any of these open-source tools is infinitely better than reusing the same password everywhere, storing credentials in a “passwords.xlsx” file on your desktop, or relying on the sticky note you might be looking at right now. If you are part of a team, this is the first tool you should deploy collectively.

What about critical business access?
For shared passwords within an organization (server access, admin accounts, API keys, supplier credentials), the logic is different. It is no longer about personal convenience but business continuity. What happens if the only person who knows the root password is away? In a large defense contractor we worked with, the solution is radically low-tech: a sealed envelope in a physical safe, updated with every password change. It isn’t elegant, but it is resilient, offline, and immune to any cyberattack. For smaller organizations, shared access management sovereign solutions exist and can be hosted on your own infrastructure.

Change your browser and search engine

Firefox (Mozilla, a non-profit foundation) rather than Chrome (Google). Brave is an interesting alternative with native tracker blocking, though it remains a US-based company. For your search engine, try Qwant (French) or DuckDuckGo instead of Google Search. These are simple actions that immediately reduce the amount of personal data collected from your browsing, as well as that of your employees and your clients when they visit your premises and use your Wi-Fi. We know that changing habits doesn't excite anyone. But these browsers are faster, display fewer ads, consume less memory, and don't track your every move. After a week, no one ever looks back.

Things that take a weekend (and already change a lot)

Jitsi for your online meetings

Every meeting on Teams or Zoom passes through American servers. Your call metadata (who talks to whom, when, for how long, from where) is collected and stored under US jurisdiction. And the content itself is not spared: recordings, automatic transcripts, and summaries generated by the AI integrated into these platforms feed learning models and constitute a source of intelligence over which you have no control. For sensitive internal meetings, client exchanges, or strategic discussions, this is a risk many organizations underestimate.
Before renewing your licenses, try Jitsi Meet. Open source, encrypted, and usable without an account or installation—a simple link in the browser is enough. Send it to your next meeting participants and observe the outcome. Chances are, they won't see any difference. In fact, this is the solution on which the French government built Visio, the European alternative designed to replace Teams and Zoom for 2.5 million civil servants.

Switch your web analytics to Matomo

If your site uses Google Analytics, every visit from your clients, prospects, or constituents generates data that is sent to Google, processed in the United States, and potentially exploited for advertising purposes. This isn't just a matter of principle: since the invalidation of the Privacy Shield, several European data protection authorities (data protection requirements in the GDPR context) have ruled Google Analytics non-compliant with the GDPR. By continuing to use it, you are exposing your organization to a real legal risk. Matomo (French, open source) does the same job, is GDPR-compliant by design, and can be hosted on your own server. Your visitors' data stays

with you, period. Secure digital migration is simple and consists placing a snippet of code on your site. It takes about half a day if you are unfamiliar with it, likely less if you have a technical background, and it is a service we regularly deploy.

Check your domain name and email provider

Log in to your registrar's interface and check two things. First, ensure that the domain is properly registered in your name, and not in the name of a former service provider who could hold onto it in the event of a dispute. Second, check that the registrar itself is European. The site European Alternatives maintains a list of accredited European registrars. If you don't know what a registrar is or where to log in, that is already important information regarding your level of dependency—and exactly the kind of question that external support can untangle in a few minutes. Take this opportunity to check who actually manages your emails. If your professional addresses run through Gmail or Outlook/Exchange, every message sent and received—contracts, quotes, client data, password resets—transits through and is stored by Google or Microsoft. Your domain name and your emails are the two most critical digital assets of your organization. They are also the first things you should regain control over, and we will detail how in an upcoming article dedicated to messaging.

Audit your online services

Start by listing all the tools your organization uses on a daily basis. For each one, ask three questions: Where is the data hosted? Under which jurisdiction? And if this service disappears tomorrow, can I retrieve my data in a usable format? If the answer is "no" or if you don't know, you have found your top priority for what comes next. If your organization is larger or if your applications are numerous, this exercise becomes a full-scale audit that deserves to be structured; we will return to this in the next section. In either case, this inventory often holds surprises, and it is frequently more effective when conducted with an outside perspective that knows exactly which questions to ask to improve cyber resilience.

Raise awareness among your employees

Gather your teams for an hour and share what you have learned with them. Share the "Have I Been Pwned" results for company email addresses, the list of program and their jurisdictions, data breach statistics, and more. The goal is not to spread fear, but to foster accountability. Digital security and sovereignty are not just IT issues; they are collective responsibilities. Often, it is this shared awareness that triggers real change. Present this information in a way that your employees can replicate at home with their families. Good digital practices don't stop at the office door—and if your team members have teenagers at home, you will gain some unexpected allies.

Actions that require a plan (and likely a helping hand)

The previous actions are individual steps. Those that follow involve the infrastructure and organization of your entity. They require prior reflection, a realistic schedule, and often professional guidance. This is where we move from a civic gesture to a strategic decision.

Conduct a true dependency audit

We detailed the method in our previous article. This involves mapping every layer (hardware, operating systems, applications, cloud services, shadow IT), identifying jurisdictions, and reviewing contracts. If you performed the quick weekend inventory, you already know where the pain points are. A structured audit goes further: it quantifies risks, identifies hidden dependencies, and produces a prioritized roadmap. This is the starting point for any serious

professional support.

Take back control of your emails

Take back control of your emails. If the weekend inventory confirmed that your emails transit through American servers, this is your top priority. Transfer your domain to a European registrar, point your MX records to a server you control, and deploy a sovereign email solution. This is a project that takes a few days, not months, and we will dedicate an entire article to the available secure solutions. If you are in a hurry, contact us.

Host your data on your own server

As we showed in our previous article, a high-performance server tailored for an SME can be set up with approximately €2,000 of hardware, and it pays for itself in just a few months compared to cloud subscriptions. Whether hosted on your premises or with a European provider and managed via Open Source tools like Virtualmin and Webmin, it becomes the foundation for your emails, files, backups, and business applications. This is one of the building blocks we deploy most frequently.

Review your contracts

Every provider identified in your audit is tied to you by a contract that you likely signed without reading in detail. Check the reversibility clause (can you retrieve your data in a usable format?), data ownership (is the provider prohibited from exploiting it?), applicable jurisdiction (which court applies in case of a dispute?), and termination conditions (are there penalties, notice periods, or automatic deletions?). This task requires a legal perspective. If you do not have a lawyer specialized in digital law, now is the time to consult one. We work in partnership with firms experienced in these matters and can point you in the right direction.

What requires courage (and time)

The previous projects involve infrastructure. Those that follow involve habits. And that is where it gets tough.

Migrate your office suite

This is the subject that triggers the most resistance. After years spent on Word, Excel, and PowerPoint, asking a team to switch to LibreOffice or OnlyOffice provokes visceral reactions. Yet, for 90% of daily use cases, the transition is seamless. The real obstacle is not technical; it is cultural. Thirteen years of schooling using Microsoft tools leaves deep-seated reflexes. The key is support: not a two-hour training session on a Friday afternoon, but a long-term presence—someone who answers questions as they arise, within the actual context of the work. We will detail these technical and pedagogical approaches in a dedicated article.

Switch to sovereign infrastructure for collaboration

Google Drive, SharePoint, Dropbox, Notion, Slack, Trello, Salesforce... many organizations stack half a dozen American services to collaborate. Alternatives exist. Nextcloud for file storage and sharing. Tiki Wiki for those who want to go further: wiki, project management, CRM, forms, workflows, and even integrated messaging via Cypht—all within a single platform hosted on your own premises. The advantage of an all-in-one solution is a single server to secure, a single set of data to govern, and a single migration to Open Source solutions instead of six. We will also dedicate a full article to this topic.

The workstation: Linux or not

Let’s be honest. The choice of operating system for workstations is the most sensitive topic of the entire process. Linux is the only fully sovereign option. Ubuntu or Linux Mint for ease of use, Fedora for structured professional environments. The French National Gendarmerie runs over 103,000 workstations on GendBuntu, and the State has just announced the DINUM digital migration. But the reality on the ground is that some professions depend on software that doesn't exist on Linux: graphic designers using Adobe, accountants with certified software, CAD engineers. I use macOS daily myself. Acknowledging this doesn’t discredit the approach: it shows we live in the real world. The essential thing is to protect what matters most: the server, the data, the emails, and the collaborative tools. A macOS or Windows workstation connecting to a sovereign infrastructure is already 80% independent in its usage. Start with the server. The workstation will follow—or not—depending on your actual constraints.

Mobile devices: accepting the limits

iOS and Android share 99% of the market. There is no mainstream alternative. But you can limit the damage: Signal instead of WhatsApp, Nextcloud instead of iCloud or Google Drive, Firefox instead of Chrome, and a local password manager rather than Google Keychain. It’s not a perfect solution, but it is a significant reduction of your exposure surface. And above all, apply the same rules to your mobile devices as your workstations: no sensitive professional data on an unsecured personal phone.

In a now-famous security lapse, the Strava fitness app inadvertently revealed the locations of secret US military bases and patrol routes in conflict zones like Syria and Afghanistan. By simply publishing a "heat map" of popular running routes, the company exposed the precise perimeters of outposts that didn't even appear on public maps—all because soldiers were jogging with their tracking on. There was no hacking and no cyberattack; it was just a fitness app and a default privacy setting. Your organization might not be a secret military base, but the mechanism of exposure is exactly the same.

Protect what you have reclaimed

Regaining control of your infrastructure without securing it is like moving into a brand-new house and leaving the front door wide open. The previous sections were about sovereignty; this one is about survival. And cybersecurity posture is a specialized skill.

As we detailed in our previous article on breaking digital dependency and noted earlier with the alarming figures from early 2026, attacks are now automated, constant, and indifferent to whether you are a multinational or a small business. The solution rests on three inseparable pillars: real-time monitoring that alerts you before an incident turns into a crisis; geographic access filtering to block the noise and intrusion attempts before they even reach your server; and regularly tested offsite backups, because as we've warned before, a backup that has never been verified is nothing more than a hope. This isn't a project to be improvised on a Sunday afternoon. It is a cohesive system that must be designed, deployed, and maintained by a partner who knows your infrastructure and monitors it over the long term.

And tomorrow: protecting your data and your business in the age of AI

There’s one topic we’ve only touched on—and it deserves an article of its own. How many of your employees are already using ChatGPT, Copilot, or Gemini with client data, internal documents, or strategic information? Each prompt can potentially feed models hosted under foreign jurisdictions, with little to no visibility on how that data may be reused.
And that’s only one side of the issue. Your public content, documentation, and hard-earned expertise are already being scraped and absorbed by AI systems—sometimes to train models that may ultimately benefit your competitors.
Sovereign infrastructure alternatives are emerging and gaining maturity to improve cyber resilience. Open Source models such as Mistral or LLaMA can now run on your own infrastructure, locally, ensuring that no sensitive data ever leaves your environment. This is not a distant future—it’s an operational choice you can start making today. We’ll explore this in depth in an upcoming article.

What comes next is up to you

Between government initiatives, new regulations, and the surge in cyber threats, 2026 marks a clear turning point. Digital sovereignty is no longer a niche concern for experts—it’s a daily operational challenge for every organization, regardless of size.
The gap between theory and reality is closing fast. The only question is: will you stay dependent, or take back control?

What we’ve shared in this article are not miracle sovereign and open Source solutions. They are first steps—practical actions that any organization can take, at its own pace. Some take an hour, others require planning and support. All of them help reduce your exposure and strengthen your independence and they need to be strategized together, because digital sovereignty without cybersecurity and data protection is only an illusion.

In the coming articles, we’ll break down each building block with the same hands-on approach:

- Email: taking back control of your communications, from DNS migration to deploying a sovereign solution with Cypht and Tiki Wiki
- Office European alternatives: technical and organizational methods for a smooth transition to LibreOffice or OnlyOffice
- Collaboration and storage: Nextcloud, Tiki Wiki, and how to replace half a dozen US-based SaaS tools with a platform you fully control
- Analytics and web: Matomo, sovereign hosting, and SEO strategies beyond Google
- Everyday cybersecurity: digital hygiene, user best practices, and what everyone can do
- Sovereign AI: protecting your business data and deploying AI locally on your own infrastructure
- For individuals: what anyone can do at home, for themselves and their family

If you don’t want to miss these publications, subscribe to our newsletter. No spam, no overwhelming frequency—just a signal when a new article is released or when something important happens in the world of digital sovereignty. And if this article has helped you identify urgent issues—or if you simply don’t know where to start—that’s exactly what we’re here for.