KELDARX

01

WHITE PAPER · B2C

Your data belongs to you. Really?

What Big Tech isn't telling you about your digital life

Pascal NAPARTY · CEO & Founder, KELDARX

June 2026 · Reading time: 12 min

Key Takeaways

‣ You use dozens of Cloud applications that store your data on servers you don't control.

‣ The U.S. CLOUD Act (2018) authorizes American authorities to access your data, even when hosted in Europe.

‣ Your personal data represents considerable economic value — exploited by platforms, not by you.

‣ Three major risks threaten your digital life: captivity, exposure, and fragmentation.

‣ The GDPR, Quebec's Law 25, and the Cyber Resilience Act grant you rights. Exercising them remains complex in practice.

‣ Local-First architecture now makes individual digital sovereignty possible — without technical expertise.

‣ KEY is the first platform that gives you physical and mathematical ownership of your digital assets.

Introduction: The illusion of digital ownership

When did you last read the terms and conditions of the last app you installed?

Most of us never do. And it is precisely on that silence that one of the most discreet value transfers in modern economic history rests.

Every day, you create, share, and store data: photos, documents, messages, geographic locations, consumption habits, health data, financial information. You have the impression that this data belongs to you. It's in "your" Cloud, on "your" phone, in "your" account.

The legal and technical reality is different.

By clicking "I agree," you have granted extensive rights over that data to companies whose shareholders, servers, and government contracts you know nothing about.

This white paper explains what that means in concrete terms — and how to take back control.

1. What you agreed to without reading it

The world's most widely used digital platforms share a common business model: you are the product.

This is not a metaphor. It is a documented commercial reality.

Your data fuels advertising targeting algorithms, AI training models, and behavioral analyses sold to third parties. The value of your data does not disappear when your session ends. It accumulates, cross-references, and monetizes.

What you have really accepted

By accepting the Terms of Service (ToS) of most consumer platforms, you have typically granted:

- The right to use your data to "improve services" - wording that covers AI training.
- The right to share your data with unnamed "partners."
- The right to retain your data after you close your account.
- The right to amend these terms unilaterally, with a simple notification.

The Cloud Act: When your data becomes American

In 2018, the United States passed the **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act). This law authorizes U.S. authorities to demand access to data stored by U.S. companies, **regardless of the physical location of the servers**.

Your data hosted on Google Drive, iCloud, Dropbox or OneDrive — even on European servers — is potentially accessible to U.S. authorities without prior notification [1].

Both the French Council of State and the Court of Justice of the European Union have identified this law as incompatible with European fundamental rights. Legal tension persists, with no final resolution to date.

KELDARX Perspective

It's not a question of whether you have something to hide. The question is whether you accept that others decide for you what belongs to you.

2. Your data has a value you don't perceive

The personal data economy is one of the most profitable industries of the twenty-first century.

The paradox of value

You produce valuable raw material. You deliver it free of charge. Others monetize it. You receive nothing in return.

This model is made possible by two mechanisms:

1. **Invisibility** — you don't see your data "going"
2. **The value of immediate access** — you accept the contract because the service is convenient now

This model has a concrete number. According to Meta Platforms, Inc.'s 2023 Annual Financial Report — mandatorily published with the U.S. stock exchange authorities and publicly available [2]:

Region	Revenue generated per user per year
United States & Canada	~$210-$220
Europe	~$75-$80
Asia Pacific	~$18-$20
Rest of the world	~$13-$15
World average	**~$40-$45**

This revenue is generated **almost exclusively through targeted advertising**, which is itself fueled by the detailed analysis of your personal data and online behavior.

In Europe, your digital life is worth around **$75-80 per year to Meta**. You don't get a penny from it. You pay with your privacy.

The crisis of confidence is documented

According to the **Edelman Trust Barometer 2025**, trust in big tech companies is at an all-time low in developed countries [3]. Users are increasingly aware of the exploitation of their data — but feel that they have no viable alternative.

This feeling of powerlessness is the main barrier to regaining control.

> KEY is designed to remove this barrier.

The Invisible Captivity

Your photos on iCloud. Your emails on Gmail. Your documents on Google Drive. Your contacts on your Android phone. Each service makes you a little more dependent — and a little harder to leave.

This phenomenon has a name in the industry: **vendor lock-in**. It is not accidental. It is designed.

3. The 3 risks you underestimate

These risks have concrete consequences for your daily life and your digital future.

Risk 1 — Captivity with no emergency exit

What happens if a platform deactivates your account? If it increases its prices? What if it shuts down the service?

These scenarios are not hypothetical:

- Accounts are deactivated without notice for alleged violation of the Terms of Use.
- Services are unilaterally stopped (Google+ closed, Google Stadia abandoned, Google Photos modified).
- Cloud subscription prices have increased significantly between 2022 and 2025 [4].

When this happens, is your data recoverable? In what format? How long will it take? The answer depends on the goodwill of a company whose interests are not aligned with yours.

Risk 2 — Exposure without your knowledge

Your data is not only collected. It can be exposed.

Data breaches affect hundreds of millions of users every year. Compromised data is resold on underground markets, cross-referenced with other sources, and used for identity fraud.

Regulation is progressing:

- The **European GDPR** (2018) imposes strict obligations on companies and gives you rights (access, rectification, erasure, portability) [5].
- **Law 25** (2023) imposes penalties of up to **$25 million or 4% of global sales** [6].
- The **Cyber Resilience Act** (CRA, European Commission, 2024) imposes security standards on software marketed in Europe [7].
- The **NIS 2 Directive** makes managers criminally liable in the event of negligence on data security [8].

These texts protect your rights. They do not repair a data breach that has already occurred.

> **KELDARX Perspective**
>
> Regulatory compliance protects companies from penalties. It does not protect your data. Protecting your data starts with you.

Risk 3 — Fragmentation and loss of control

The third risk is the most insidious because it is gradual.

Every new app installed. Each new service activated. Each new permission granted. Your digital life is fragmenting into dozens of silos owned by as many different companies.

As a result, you no longer know where your data is, who is accessing it, and what is happening with it. This fragmentation has a real cost:

- Time wasted finding information dispersed between several tools.
- Multiple versions of the same document impossible to reconcile.
- Impossible to reconstruct a coherent personal history.
- Increasing administrative mental load.

The figures are overwhelming:

- According to the **McKinsey Global Institute**, knowledge workers spend an average of **1.8 hours a day** — or nearly **20% of their workweek** — searching for information, documents, or soliciting colleagues to find the right data [9].
- The IDC (International Data Corporation) estimates this time at 2.5 hours a day, or 30% of working time, often without finding the information they are looking for [10].
- **Gartner** points out that nearly **half of professionals** admit to regularly having difficulty locating the right document at the right time — leading to recreating documents that already exist [11].

This is not a personal organization problem. It is the direct consequence of a digital life fragmented across dozens of disconnected silos.

4. Digital sovereignty is no longer just for states

For a long time, digital sovereignty was a geopolitical concept. States were debating the hosting of their public data and their independence from American hyperscalers.

This debate is now descending to the level of the individual.

Three disruptions converge simultaneously to make personal digital sovereignty possible.

Disruption 1 — Regulatory maturity

The GDPR, Law 25, the CRA, and the European Data Act converge on a fundamental principle: **your data belongs to you, and you have the right to control it**.

These texts are not just obligations for companies. These are rights for you:

- **Right of access:** obtain a copy of all data held about you.
- **Right to rectification:** to correct inaccurate data.
- **Right to erasure:** request the deletion of your data.
- **Right to portability:** recover your data in a reusable format.
- **Right to object:** refuse certain uses of your data.

The problem is that exercising these rights remains complex in practice. Most individuals never do. KEY automates this process.

Disruption 2 — The technological maturity of Local-First

Local-First **architecture** is a technology paradigm that reverses the dominant cloud model: your data is stored and processed first on your own devices. Cloud synchronization is optional and under your full control.

This approach was not feasible on a large scale five years ago. Advances in lightweight databases (SQLite), strong embedded encryption, and selective synchronization now make it available to the general public.

The **WEF Global Risks Report 2025** identifies reliance on foreign software infrastructure as a systemic vulnerability [12]. What states are beginning to address for their own sovereignty, individuals can now address for themselves.

Disruption 3 — The demand for sovereignty as a standard

The figures are unequivocal:

- **81%** of adults feel they have little or no control over the data collected by tech companies [13].
- **79%** of users are concerned about how companies use the data they collect [13].
- **71%** of respondents are concerned that the collection and monetization of their personal data is a risk to their privacy [14].
- The **Edelman Trust Barometer** has recorded a consistent decline in public trust in social networks and major technology platforms for several years. Privacy protection and cybersecurity are now users' absolute priorities for restoring that trust [3].

The demand for digital sovereignty exists, massive and documented. Until now, no suitable solution existed.

> **KELDARX Perspective**
>
> Individual digital sovereignty is not a tech-savvy luxury. It's the next logical step in protecting your fundamental rights in the digital age.

5. Regaining control without being an engineer

The main objection is often *"it's too technical for me."*

This objection was legitimate in 2015. It is no longer in 2026.

No-code is a game-changer

Modern data management platforms eliminate the technical barrier. You don't need to understand how a database works to use one. You don't need to configure a server to benefit from a Local-First architecture.

The analogy is simple: you drive a car without understanding the combustion engine. You use a smartphone without programming an app. You can manage your data sovereignly without being a developer.

What concrete digital sovereignty means

Big Tech model (today)	KEY model (tomorrow)
Your data on their servers	Your data on your devices
Unilaterally revocable access	Permanent and unconditional access
Monetization of your behaviors	No commercial exploitation
Fragmentation into dozens of silos	Sovereign centralization
Third-party dependent compliance	Native and verifiable compliance

KEY: the platform for individual sovereignty

KEY is built on three non-negotiable pillars:

1. **Local-First — physically with you by default — on-premises** or Cloud as needed
2. **No-Code** — no technical skills required for complete governance of your data
3. **Open architecture** — no vendor lock-in, full portability guaranteed

> KEY is not an alternative to an existing cloud service. It's a paradigm shift: you go from being a tenant of your data to an owner.

Conclusion: The question you should ask yourself today

Is your data safe? Probably not as much as you think.

Do you have control over your data? Probably less than you think.

Can you regain this control without relearning everything? Yes — and that's precisely what KEY makes possible.

Digital sovereignty is not a technical issue. It's a matter of choice.

The regulatory world (GDPR, Law 25, NIS 2, CRA) gives you the rights. Technology (Local-First, no-code) gives you the tools. KEY gives you the platform.

All that's missing is your decision.

Sources & References

[1] CLOUD Act (Clarifying Lawful Overseas Use of Data Act), U.S. Congress, 2018 — congress.gov

[2] Meta Platforms, Inc. — Form 10-K 2023 (annual report filed with the SEC) / Earnings Releases 2023 — investor.fb.com

[3] Edelman Trust Barometer 2025 — edelman.com/trust/2025-trust-barometer

[4] MacRumors — "Apple Hikes iCloud+ Subscription Prices in Many Countries Around the World" (June 2023) — macrumors.com · Microsoft — Announcement of Microsoft 365 Personal and Family price increase (October 2024)

[5] GDPR — Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016, Art. 15-21 — eur-lex.europa.eu

[6] Act respecting the protection of personal information in the private sector (Law 25), Government of Quebec, 2023 — legisquebec.gouv.qc.ca

[7] Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, European Commission — digital-strategy.ec.europa.eu

[8] NIS 2 Directive (EU 2022/2555), European Commission — digital-strategy.ec.europa.eu

[9] McKinsey Global Institute — "The social economy: Unlocking value and productivity through social technologies" — mckinsey.com

[10] IDC (International Data Corporation) — Study on information search time in the workplace — idc.com

[11] Gartner — Survey on document location in the workplace — gartner.com

[12] WEF — Global Risks Report 2025, World Economic Forum — weforum.org/publications/global-risks-report-2025/

[13] Pew Research Center — "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" — pewresearch.org

[14] YouGov & Amnesty International — Multinational survey on surveillance and digital privacy — amnesty.org

All trademarks, product names and logos mentioned herein are the property of their respective owners. Their mention is purely informational and does not constitute any form of affiliation or endorsement.

About KELDARX

KELDARX develops KEY, the first platform that gives everyone the technological capabilities that only large enterprises could afford.

KEY is built on three pillars: Local-First architecture (your data on your devices by default — on-premises or cloud as needed, always under your control), mathematical determinism (100% predictable and verifiable results — AI assists, it never decides), and an obfuscated database that makes your digital assets invisible to unauthorized access — ransomware included. Its upcoming business solutions will enable individuals and businesses to share the same sovereign infrastructure to control their digital lives for the first time.

Your Digital Life. Your rules.

Pascal Naparty — CEO & Founder, KELDARX

Take the next step

Join the KEY waitlist — be among the first to take back control of your digital life.

→ keldarx.com

For any questions: **contact@keldarx.com**