THE STRATEGIC IMPORTANCE OF DIGITAL SOVEREIGNTY IN 2026

By Alexandre Grellier, CEO, Drooms (www.drooms.com)

Digital sovereignty has become a priority for organisations in 2026 as concerns over data privacy, data protection, and geopolitical risk intensify.

Digital sovereignty has become a priority as concerns over data privacy, data protection, and geopolitical risk intensify. The concept centres on giving data owners full control over their digital assets, infrastructure, and the legal frameworks governing them. While Europe leads demand for sovereign solutions, interest is rising globally as cyberthreats and geopolitical tensions grow.

In 2026, digital sovereignty moved from EU policy papers into the day to day decisions of Data Protection Officers (DPOs), Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs). At the very moment when an organisation is sharing its most sensitive information – during an M&A deal, asset sale, refinancing or fundraising – it needs to ask the simple question: is the platform that stores and processes our data and the company behind it fully and exclusively subject to European jurisdiction?

Digital Sovereignty: What It Means and Why It Matters in 2026

Digital sovereignty is the ability of individuals, companies, and states to act and make independent decisions in the digital world without relying on foreign providers. While definitions can be abstract, for dealmakers and security leaders the concept centres on three practical questions:

1. **Data sovereignty**
   Who can access your data, under which laws, and where is it stored and processed?
2. **Infrastructure sovereignty**
   Who owns and operates the underlying infrastructure - data centres, cloud stacks - and which jurisdiction can compel them to act?
3. **Technology sovereignty**
   Who develops and controls the software and AI processing your data, and are there external services or models you cannot fully see or govern?

These questions apply not only to the technology itself but also to the legal entity behind it. A platform may sit in an EU data centre yet still be controlled by a non European company subject to foreign law. True digital sovereignty requires credible answers across an organisation's entire digital estate, including specialist tools used for due diligence, Q&A, document review, and deal collaboration.

A recent case in France illustrates how platform origin and jurisdiction can collide with sovereignty expectations.

A French Senate Reminder

In June 2025, during a hearing of the French Senate's commission of inquiry on public procurement, Microsoft France's head of legal and public affairs acknowledged that the company could not guarantee that data stored in France would be shielded from US judicial requests. When asked whether Microsoft would hand over data hosted in France if ordered by an American judge, he confirmed that the company would comply once internal review steps were exhausted.

This reinforced a key point: the US CLOUD Act follows the provider, not the server location. As a result, using US controlled cloud stacks for sensitive workloads such as health data platforms, public sector systems, or "trusted cloud" initiatives has become increasingly controversial in France. The same logic applies to private M&A, real estate, and financing deals: "EU-hosted" alone does not deliver digital sovereignty if the platform is governed by non EU law.

Another key consideration is whether the AI being used is GDPR compliant and doesn't compromise digital sovereignty.

As organisations across the EU and UK increasingly adopt AI solutions, ensuring GDPR compliance and appropriate data residency has become a crucial factor. Some providers have started to connect external AI tools such as Claude, ChatGPT, and Copilot, directly into their data rooms, enabling the use of these tools for data analysis. While it may seem like a quick win solution, connecting external AI tools into a data room may expose confidential data to public clouds and data sharing, which can pose significant risks for data leaks.

It is crucial to understand the specific policies and practices of each tool and how they run inside the data room – whether they are built in or connected – to ensure compliance with digital sovereignty requirements. There is a significant risk in exposing your confidential information every time you ask an external AI tool a question, to servers you don't control, in a jurisdiction that isn't compliant. Users should therefore carefully consider the data-handling policies of the platforms they choose for their transactions – including their AI.

Understanding GDPR and Data Residency

GDPR imposes stringent rules for handling personal data within the EU and UK. It requires transparency, user consent, robust security, and clear arrangements for where data is stored and processed. For organisations adopting cloud-based AI, compliance with GDPR and local data protection laws is essential.

For regulated organisations, the headline isn't "which model is most compliant", it is which option provides the clearest evidence trail with the least operational risk.

Are you using the right solution for your GDPR requirements?

Ensuring GDPR compliance and proper data residency isn't optional; it is essential for organisations adopting AI across Europe and the UK. Organisations must thoroughly understand which platforms, and the integrated LLM solutions, align best with their compliance and business needs.

Why Digital Sovereignty Is a Priority Now

Developments such as the above have pushed digital sovereignty to the top of the 2026 agenda for European policymakers and CIOs. Control over data, compute, and cloud infrastructure is now seen as essential for economic competitiveness, democratic resilience, and geopolitical autonomy.

Two structural issues dominate EU discussions:

- A small number of non European hyperscalers still control most of the EU cloud market - around two thirds by some estimates.
- Critical workloads in the public sector, financial services, and strategic industries often run on platforms governed by foreign law.

In response, Europe is seeing:

- Accelerating investment in sovereign cloud initiatives, with spending expected to grow sharply.
- Major US providers launching EU sovereign cloud offerings operated by EU entities with stricter controls.
- Guidance urging CIOs and CISOs to treat sovereignty as part of digital resilience and cloud strategy, not a niche compliance topic.

For sectors where confidentiality is central - M&A, real estate, private equity, banking, energy, and defence - this shift directly affects the tools used to store and share the most sensitive information: data rooms.

The Legal Backdrop: CLOUD Act, GDPR, Schrems II

The urgency around sovereignty stems from the collision between European data protection rules and extraterritorial foreign laws.

US CLOUD Act

Allows US authorities to compel providers under US jurisdiction to hand over data within their "possession, custody or control," regardless of where the data is physically stored.

GDPR and Schrems II

GDPR (notably Article 48) and the CJEU's Schrems II ruling impose strict conditions on foreign access to EU personal data and highlight concerns about disproportionate US surveillance powers.

In practice:

- Using a US headquartered or US controlled cloud or SaaS provider creates a structural tension: they may be obliged to respond to US orders even for data held in EU data centres.
- "EU hosted" is insufficient if the provider is not European or uses non European subprocessors.

For high stakes deals involving confidential documentation and investor information, this is not theoretical - it affects the platforms used for due diligence, Q&A, and post deal archiving.

Why This Matters for Your Next Transaction

During a transaction, an organisation is effectively exposing its most confidential information to a third party platform. Typical workflows include:

- Centralising all due diligence materials - financials, contracts, regulatory and technical reports - in a data room.
- Allowing buyers, lenders, counsel, and advisors to collaborate, ask questions, and leave notes.
- Using integrated communication tools to clarify issues and share links internally.
- Archiving the final state of the data room at closing for legal and regulatory purposes.

At each stage, sovereignty questions arise:

- Is your platform provider European established and European controlled, or exposed to extraterritorial legislation like the CLOUD Act?
- Are deal related communications integrated within your sovereign data room, or are you using tools governed by non European jurisdictions?
- Is any AI used in search, translation, or document analysis run by external providers you cannot fully audit?

If the answer is "we don't know" or "yes, they are US based," your next transaction may rely on tools misaligned with the EU's sovereignty direction. Platforms developed fully in house within Europe offer a clearer path to digital sovereignty.

Why Platform Origin Matters More Than Server Location

For years, the key due diligence question was: "Are our servers in the EU?" In 2026, this is no longer decisive. The more important question is: "Under whose laws does our platform operate?"

Sovereign cloud guidance highlights two operating models:

1. **Full EU isolation model**
   The provider is fully European owned, European operated, and governed solely by EU law (or equivalent).
2. **Guardrail sovereign model**
   Non European cloud companies offer European specific regions with additional controls but remain under a non European parent.

Both models have roles in broader cloud strategies. But for highly sensitive workloads like transaction

platforms and data rooms, full European isolation offers three advantages:

- No primary exposure to foreign surveillance or disclosure laws.
- Simpler legal analysis for DPOs and counsel - one primary legal regime instead of overlapping ones.
- Clearer signalling to regulators, investors, and counterparties about risk posture.

Server location still matters, but sovereignty in 2026 is fundamentally about platform origin, ownership structure, and control over the technology stack - not just the postal code of the data centre.

Practical Steps: Making Digital Sovereignty Part of Your Deal Playbook

If you are planning a transaction in the next 12–18 months, here are concrete steps to integrate sovereignty into your process.

1. Put sovereignty on your RFP and due diligence checklist

Ask any deal platform:

- Where is your organisation headquartered, and under which jurisdictions do you fall?
- Are you owned or controlled by any non European entity?
- Where are your primary and backup data centres, and who operates them?
- Do you use any non European subprocessors?
- How is your AI trained, and is it developed in house?
- How do you handle government or law enforcement requests from outside of Europe?

2. Treat AI as part of your sovereignty architecture

As AI becomes embedded in due diligence, treat it as part of your sovereignty posture. Key questions:

- Where does the AI run - on which cloud and in which region?
- Is any of your data sent to external models or used to train them?
- Can you demonstrate to regulators or counterparties that your AI enhanced due diligence respects EU data protection and sovereignty standards?

In 2026, many organisations are realising that "AI everywhere" is incompatible with "control nowhere." The winning model is AI developed in house and embedded within a sovereign, well governed platform.

Looking ahead: 2026 as a turning point

As regulatory expectations tighten, the strategic question becomes unavoidable: if you are serious about shielding your next transaction from foreign jurisdictional exposure, there is only one credible direction to take. Migrating to a European platform purpose-built for secure, compliant, and sovereignty-aligned dealmaking ensures that your organisation is not only compliant today but structurally prepared for the decade ahead. ■

ABOUT THE AUTHOR

Alexandre Grellier, CEO of Drooms, (www.drooms.com) a leading European-owned and sovereign due diligence platform, has been managing the company since 2003 and has played a key role in the development of international presence. A former Lehman Brothers lawyer in Frankfurt and London, he trained at Fresenius AG, studied law in Augsburg, and began his career at Commerzbank.