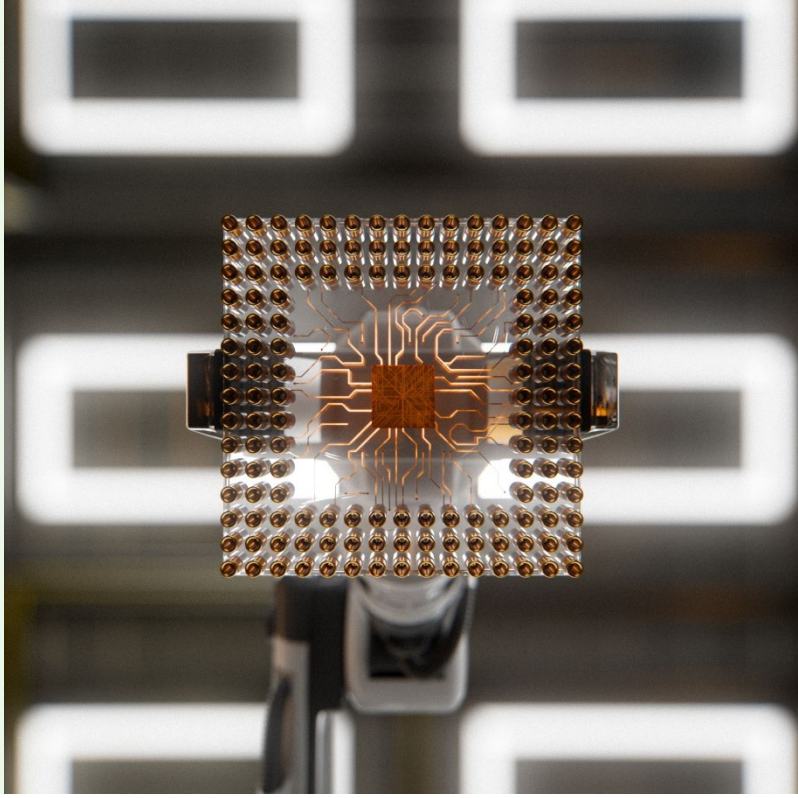
Clifford Chance

Deconstructing and achieving digital sovereignty for Europe

20 February 2026



There are growing calls in Europe for digital sovereignty. This article examines what that actually means, how it can be realistically achieved without compromising on the ability to innovate, and what organisations are already doing to make it a reality.

Cloud adoption has been accelerating as organisations are asked to deliver more with less. The public release of OpenAI's ChatGPT in November 2022 crystallised that shift, ushering in a new era of generative AI, intensifying demand for the technology and the data centres that power it. With this has come an increased focus on who is providing Europe with that technology.

Recent global turbulence, exemplified by the US-China trade war and periodic strains in US-EU relations, has thrust digital sovereignty from a niche concern to a mainstream policy issue. European leaders are worried about over-reliance on foreign tech companies for critical digital infrastructure. Some fear that political or legal directives issued outside Europe could force restrictions on how cloud and AI services are delivered in the EU, raising questions around continuity and resilience. Long-standing concerns about US government access to EU user data (e.g., under the CLOUD Act) have also resurfaced.

The confluence of these factors has made "digital sovereignty" a rallying cry in Europe's policy circles. This is driven by a desire for greater digital self-determination and autonomy, including building a competitive domestic industry and indigenous capacity (as underscored by the Draghi report) – all important objectives, yet how to achieve them remains hotly debated.

Sovereignty policy momentum is building

Sovereign sentiments already appears in EU instruments – for example, DORA which addresses concentration risk as part of its resilience regime – and legislative activity is only accelerating. Alongside constructive proposals, such as the Quantum Act and European Innovation Act, to support and invest in local technology and infrastructure capabilities – more interventionist ideas are circulating, including the Commission's open letter to build support for a "buy European" preference in public procurement and calls from groups such as the Open Markets Institute to

use the Digital Markets Act and the Data Act more aggressively to rein in hyperscalers. The European Commission's new Cloud Sovereignty Framework has further signalled a more systematic approach to how sovereignty will be evaluated and measured across the EU.

Europe is at an inflection point. These sovereignty concerns can, and in some cases already do, affect European innovation. Now is the time to have a frank conversation – about what these concerns are, sort fact from fiction, and understand how we can collectively navigate our way through them.

Part one: What does digital sovereignty actually mean?

In the cloud and AI context, "sovereignty" is widely used but not well defined or consistently understood. It is often invoked as a catch-all for concerns ranging from cybersecurity and privacy to industrial competitiveness and digital autonomy. Because it can mean very different things to different stakeholders, it has been hard to get to the crux of the issue – and therefore difficult to identify a path forward.

The "absolute sovereignty" ideal – and its costs

One extreme view is autarky: Europe achieves digital sovereignty only by eschewing non-European tech entirely – i.e., using exclusively home-grown cloud and AI solutions, hosted in sovereign data centres, with domestically built chips and software. This approach is neither realistic nor desirable. The turn to open source in the current debate (e.g., the Commission's call for evidence on open-source digital ecosystems), as a way of achieving sovereignty, also underplays the gap between theory and practice. Viewing open source as the "solution" ignores, for example, licence terms' incompatibility with sovereignty objectives, potential security issues, functionality drawbacks, and total cost of ownership factors (deployment, integration, patching, ongoing maintenance costs) all of which need to be considered.

Today's leading cloud and AI platforms benefit from massive economies of scale and sustained investment (over a combined $650 billion announced this year alone) and have established sophisticated, 24/7 monitoring and support capabilities (for example, Microsoft processes around 100 trillion security signals per day across its global cloud and security platforms, supported by tens of thousands of engineers working on security and resilience), which are hard to replicate across fragmented technology stacks. It is important to note the extensive investment by US tech companies in Europe, including commitments to support the local tech ecosystem. Even if Europe could rebuild everything domestically, shutting out foreign tech risks cutting Europe off from state-of-the-art capabilities and further foreign investment, in turn, forcing European businesses to compete with compromised technology options. So, what is the solution?

Sovereignty is about control and resilience, not ideology

Taking a step back, at the core of this debate is really the issue of control and resilience – the ability of a nation or organisation to retain control over its data, ensure the integrity of its digital infrastructure (i.e., continued access to cloud and AI services), and to determine the legal jurisdictions that govern the provision and use of those services. In our experience, the public sector tends to frame this as "sovereignty", while private-sector organisations more often speak in terms of "resilience".

Rather than treating sovereignty as a binary, all-or-nothing / either-or concept, a more appropriate and technologically accurate approach is to

look at sovereignty as a spectrum – degrees of which can be achieved by controls that can be applied and dialled up or down according to risk and what is required. These controls can broadly be implemented or achieved on three axes: contractual commitments, physical infrastructure investments and technological measures. The choice and intensity of these controls should in turn be guided by a proportionate risk assessment aligned to the sensitivity, criticality and regulatory context of the dataset and workload.

Part two: The contractual, physical and technological levers of control?

The cloud today is not the cloud of a decade or even two years ago. That is important to stress, as our observation is that sovereignty and data access concerns are often driven by outdated assumptions and misperceptions that overlook modern architectures and control tools and options that enable more effective control.

Contractual commitments

Hyperscalers are adopting contractual terms that keep customer data in Europe and commit to contesting any government orders that would suspend EU operations or compel access to EU data. Some, such as Microsoft, have committed to using all available legal avenues, including litigation, to uphold these obligations. Taken together with clearer notification and transparency practices, these undertakings substantively address concerns around the U.S. CLOUD Act and data-access (noting that even local European companies may receive an order under the CLOUD Act if they are subject to U.S. jurisdiction, for example, if they have U.S. operations or representatives), providing European public- and private-sector users with concrete, auditable safeguards.

Physical infrastructure

Cloud providers are significantly expanding their European data centre footprint – alongside initiatives such as EU Data Boundary and Data Guardian arrangements – all to keep EU customer data on EU soil, subject to EU laws and accessible only by EU support personnel. They are also adopting European governance models, including pledging that their European data centres will be overseen by an exclusively European board consisting of EU nationals.

Technological measures

Providers are leaning heavily on tools such as customer-managed external encryption keys and double-key encryption, ensuring that customers retain ultimate control over access to their most sensitive data. They are also making arrangements with European partners, for example between Microsoft and Delos Cloud, to enable operational continuity should sanctions restrict cloud services in Europe.

Part three: Technology is the control solution

The effectiveness of these sovereignty levers is that they can be deployed in layers according to the sensitivity of the data or application. The more layers applied, the closer one gets to "absolute" sovereignty – but often at incrementally higher cost and, at times, reduced feature sets. Effective sovereignty is about intelligently layering these safeguards based on need, rather than a blanket rejection of foreign technology.

Data governance is the "how"

Recognising this, we see merit in shifting the conversation from the abstract notion of sovereignty to a practical one of data governance and classification. All data is important, but not all data necessitates the same level of protection – or the same level of friction and cost.

A proportionate, risk-based approach should guide where a given dataset or workload sits on the sovereignty spectrum and which layered controls to apply. It is also essential to take a holistic view and not overweight low-probability "doomsday" scenarios at the expense of what can be practically achieved when applying the sovereignty levers.

Viewing this through the lens of resilience rather than sovereignty, private-sector clients (especially those in highly-regulated areas like financial services), have long understood that the right technology can actually enable security and continuity, and have developed sophisticated data governance frameworks to support its use. We note a persistent challenge when relying on data governance has been the operationalisation of these frameworks. Interestingly, AI is beginning to close that implementation gap by automating data classification and policy enforcement at scale, often delivering better data classification outcomes.

The bottom line – not 'either-or', but both

Sovereignty is ultimately about control – of data, operations and governing law. Sophisticated providers are working to achieve this through a calibrated mix of contractual commitments, local infrastructure, and technical controls, delivered by both EU and non-EU technology – suggesting that it is not an either-or choice. A pragmatic model is one that pairs home-grown capability with access to best-in-class global services under clear controls – based on an understanding that policies that promote European innovation should enable, not hinder, the use of the latest technology, no matter where it is from. Deployed correctly, modern cloud and AI can enhance resilience, keeping Europe plugged into innovation – on Europe's terms.

Part four: A call to action

A partnership approach to innovation

A change of mindset is needed – turning the focus from "which country does the solution come from?" to "which controls do we have?" Tech companies must continue to acknowledge European concerns and adapt their services towards greater flexibility and customer control and choice. Providers should also double down on education and transparency about how their contractual, physical and technical measures advance European sovereignty objectives, and how those controls are tested, audited and supported in practice.

In parallel, organisations should adopt data governance frameworks fit for the digital age and operationalise them with automation and AI – giving them the fidelity to decide, and enforce, what data goes where and which controls apply. From a European standpoint, it is also important to recognise that data centres are not on wheels: infrastructure commitments by large technology companies are in fact commitments to Europe and to local investment – job creation, upskilling, and collaborating with European SMEs to help them grow.

In this spirit, the newly launched Trusted Tech Alliance (TTA) is a welcome, concrete step: unveiled at the Munich Security Conference by leading companies across the tech stack, including Microsoft, Google, AWS, SAP, Ericsson, and ASML – the TTA commits members to five verifiable principles: transparent corporate governance and ethical conduct; operational transparency, secure development and independent assessment; robust supply-chain and security oversight; an open, cooperative and resilient digital ecosystem; and respect for the rule of law and data protection. These cross-border commitments are designed to build trust irrespective of supplier nationality and are a promise to work with governments and customers to couple emerging technologies with public confidence, jobs and growth.

With a partnership mindset and controls-based approach that bridges EU and non-EU technologies, Europe can achieve digital sovereignty that is real – not just symbolic – in a way that is both innovative and practical.

Clifford Chance Tech Policy Unit

At Clifford Chance's Tech Policy Unit, we are committed to being at the forefront of this sovereignty and resilience conversation, helping bridge the gap between technology providers, regulators and end-users. We are engaging with industry and policymakers to test assumptions and develop practical solutions that address legitimate sovereignty concerns while preserving the benefits of a connected digital economy. We believe this balanced perspective is crucial – rather than let rhetoric dictate the way forward, it's time to double down on dialogue and cooperation.

Jonathan Kewley
Partner and Chair of the Global Tech Group, London

jonathan.kewley
@cliffordchance.com
+44 2070063629

Phillip Souta
Global Director of Tech Policy, London

phillip.souta
@cliffordchance.com
+44 2070061097

Monika Zdzieborska
Counsel, London

monika.zdzieborska@cliffordchance.com
+44 2070061468

Andrew Cooke
Director - Technology Policy & Advisory, London

andrew.cooke
@cliffordchance.com
+44 2070061332

Dessislava Savova
Partner, Head of Continental Europe Tech Group, Paris

dessislava.savova
@cliffordchance.com
+33 144055483

Dr. Holger Lutz
Partner, Frankfurt

holger.lutz
@cliffordchance.com
+49 69 7199 1670

Dr. Tobias Born
Counsel, Frankfurt

tobias.born
@cliffordchance.com
+49 69 7199 1386

Alexander Kennedy
Knowledge Director – CE Tech Group, Paris

alexander.kennedy
@cliffordchance.com
+33 144055184

Anna Carrier
Head of EU Tech Policy, Brussels

anna.carrier
@cliffordchance.com
+32 25335048

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2026

Clifford Chance LLP is a limited liability partnership registered in England and Wales under no. OC323571. The firm's registered office and principal place of business is at 10 Upper Bank Street, London E14 5JJ. The firm uses the word "partner" to refer to a member of Clifford Chance LLP or an employee or consultant with equivalent standing and qualifications.

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest** • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague** • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.