– March 2026 –

The 2026 Tech Sovereignty Package and its Dilemmas

Dr Monique Calisti
(CEO, Martel Innovate)

www.martel-innovate.com

Summary

The **Tech Sovereignty Package** is the flagship legislative bundle of von der Leyen's second Commission, positioned as a definitive pivot from Europe acting as a "Regulatory Superpower" to becoming a "Production Powerhouse." Led by **Henna Virkkunen**, Executive Vice-President for Tech Sovereignty, Security, and Democracy, the package is a direct operationalisation of the stark warnings laid out in the 2024 Draghi Competitiveness Report and formally adopted into EU strategy via the January 2025 Competitiveness Compass (COM(2025) 30). As a reminder, one of Mario Draghi's recommendations in his 2024 Report was to reduce the regulatory burden currently stifling EU innovation.

More precisely, in his report, Draghi emphasised that Europe's complex web of overlapping rules has created a severe "innovation gap" compared to the USA and China. To address this, the Tech Sovereignty Package is not designed to completely rewrite or add to the existing regulatory burden. Rather, it is presented as a mechanism to **rationalise and streamline existing frameworks**. By reducing the bureaucratic friction that currently restrains EU innovation, the initiative aims to systematically dismantle Europe's structural reliance on foreign technology providers while unleashing the ability of domestic firms to scale.

Following a recent update to the College of Commissioners' agenda, the package has been scheduled for adoption on 27 May 2026. The drafts reveal unique ambition. However, as Europe attempts to harmonise its laws with its industrial ambitions, the package also highlights significant legal friction, funding dilemmas, and strategic tensions that public and private organisations must navigate.

The Four Pillars of Autonomy and Critical Reflections

1. Cloud and AI Development Act (CAIDA)

CAIDA addresses a severe structural dependency: Policy groups like the European DIGITAL SME Alliance note that just three American hyperscalers (AWS, Azure, Google) control roughly 65% of the EU market. Furthermore, independent analysts at Synergy Research Group estimate their combined dominance actually exceeds 70%, leaving all European providers combined fighting for roughly 15% of their home market.

To counter this, CAIDA will establish strict **"Sovereign Cloud" labels**, requiring critical infrastructure to be protected from extraterritorial laws like the US CLOUD Act. It also aims to fast-track data centre construction, provided that facilities integrate with local energy grids.

The Strategic Tension: Friction in Policy Objectives

CAIDA creates a complex balancing act within the EU's own regulatory framework. While the EU Data Act was designed to mandate open interoperability, CAIDA's strict "Sovereignty" requirements necessitate highly secure, localised environments. In a recent open letter from CISPE (Cloud Infrastructure Services Providers in Europe), 24 European cloud CEOs urged the Commission to prevent "sovereignty-washing", demanding absolute technical and legal control requirements rather than just local server hosting. Navigating this without triggering trade disputes under the General Agreement on Trade in Services (GATS) remains a delicate diplomatic challenge.

2. Chips Act 2.0: The Next-Generation of Computing

While the original 2023 Chips Act was largely a defensive play for legacy automotive chips, Chips Act 2.0 marks a bold technological repositioning. In line with the EU's broader technology goals, the new legislation focuses funding exclusively on the next generation of computing. This means investing heavily in the world's most advanced microchips, specialised hardware designed specifically to power Artificial Intelligence (AI), and the foundations for revolutionary quantum computers.

The Strategic Tension: Aligning Manufacturing with Design Capabilities

This shift in focus is scientifically ambitious and economically complex. Europe currently lacks the local "fabless" ecosystem (companies that design chips) required to fully utilise these advanced capabilities locally. By heavily subsidising manufacturing without a simultaneous increase in European chip design, there is a risk that state-of-the-art European foundries will primarily serve as manufacturers for foreign-designed intellectual property.

3. European Open Digital Ecosystems (The Open Source Strategy)

Jointly driven by DIGIT and DG CONNECT at the European Commission, this initiative moves beyond treating open source merely as a cost-saving alternative or a licensing compliance issue. Instead, it formally positions open technologies as digital commons, which are shared, public-interest digital infrastructures that are critical to European sovereignty, democratic resilience, and cybersecurity.

According to data from the GitHub Innovation Graph, there are nearly 25 million EU developers who generated over 155 million contributions to public projects in a single year. However, as highlighted in the Open Knowledge Foundation network's formal submission to the Commission's early-2026 *Call for Evidence*, the commercial value of this massive output is disproportionately extracted by large non-EU tech companies. These foreign entities routinely package European open-source assets into highly profitable, proprietary enterprise platforms, while the underlying code remains maintained by underfunded volunteer communities.

To move from theory to reality, the EU recently approved and launched the Digital Commons European Digital Infrastructure Consortium (DC-EDIC). This legally binding consortium pools national resources to jointly fund, develop, and operate cross-border open-source infrastructure (spanning AI, cloud, and cybersecurity). The explicit goal is to ensure public administrations are not forced to default to proprietary foreign software.

The Strategic Tension: Sustainable Maintenance vs Value Extraction

Global software infrastructure cannot rely on one-off innovation grants. The strategy must establish continuous, operational funding for the maintainers of critical open-source projects. Furthermore, as these projects become foundational to European tech sovereignty, they must be protected from regulatory burnout. The Cyber Resilience Act (CRA) addressed this by introducing the "*Open Source Software Steward*" role, a tailored legal framework that allows foundations to maintain sovereign infrastructure with significantly lighter compliance obligations than commercial manufacturers. By ensuring that strict technical documentation rules (such as CRA Article 31) remain proportionate for these stewards, the EU aims to secure the digital commons without creating a regulatory frightening effect on its developers. Ultimately, executing this vision requires a massive behavioural shift in public procurement, convincing Member States to adopt a strict *"buy European / open by default"* mandate.

4. Roadmap for Digitalisation in Energy

While framed as a sustainability initiative, the Strategic Roadmap for Digitalisation and AI in the Energy Sector, scheduled for adoption in early 2026 as an evolution of the 2022 EU Action Plan, operates fundamentally as a national security and critical infrastructure defence strategy.

Following a major public consultation that concluded in late 2025, the roadmap treats energy-sector AI as high-risk infrastructure, mandating strict compliance with the NIS2 Directive and the Cyber Resilience Act (CRA). It promotes the creation of a Common European Energy Data Space, utilising artificially generated "synthetic data" to train local grid-optimising AI models without violating EU privacy laws. Furthermore, the Commission is backing the development of a highly accurate Digital Twin and a European AI Foundation Model for Energy Grids, allowing operators to run millions of locally hosted simulations to test grid resilience against cyberattacks without requiring billions in physical hardware upgrades.

The Strategic Tension: The Compute vs Climate Collision

There is a profound friction between the EU's technological ambitions and its physical energy limits. The overarching package aims to onshore massive AI computing power, yet AI data centres are projected to devour staggering amounts of electricity. To manage this tension, the roadmap aligns with the upcoming Data Centre Energy Efficiency Package, introducing a strict "Grid-Positive" mandate. For a tech provider to fast-track a new data centre in Europe, they must prove the facility offers demand-side flexibility and captures waste heat for local district heating. The strategic risk is whether these strict environmental mandates will ultimately discourage the sovereign infrastructure investments the European Commission is trying to attract.

Funding Mechanisms: The Capital Markets Dilemma

To fund these initiatives, the European Commission is attempting to streamline capital through a centralised European Competitiveness Fund. As outlined in the formal legislative proposal, this framework aims to mobilise hundreds of billions to de-risk private deep-tech investments and prevent European startups from relocating to the USA. Draft proposals suggest the EU may restrict access to these massive public funding schemes exclusively to advanced tech producers based in Europe.

The Strategic Tension: Balancing Autonomy with Investment

The capital required to scale leading-edge AI and semiconductor ecosystems is overwhelming. By legally capping foreign direct investment or limiting global tech giants from accessing European subsidies, the EU faces the challenge of funding its own market. Without a fully realised and highly liquid Capital Markets Union to replace that foreign capital, a vulnerability heavily emphasised in the 2024 Draghi Report, the Tech Sovereignty Package risks setting ambitious rules without the underlying financial mechanisms necessary to execute them at a global scale.

Strategic Recommendations – Building Architectural Resilience

True autonomy is not about waiting for regulations to take effect. It requires building architectural resilience and embedding organisations into the European innovation ecosystem today. Because the operational realities differ slightly depending on jurisdiction, leaders and decision-makers must tailor their approach.

For EU-Based Organisations

- **Adopt an "exit strategy" by design:** Use **Infrastructure as Code (IaC)** to ensure your entire stack can be rapidly redeployed to an EU-native provider if CADA compliance conditions or geopolitics shift suddenly.
- **Implement "Hold Your Own Key" (HYOK) encryption:** Ensure that encryption keys for data stored on global hyperscalers are managed by an independent, EU-based cybersecurity firm to legally insulate your infrastructure from the US CLOUD Act.

- **Engage with Digital Commons and EU innovation ecosystems:** Formalise how your organisation consumes and contributes to open source. Beyond internal governance, actively partner with EU-funded initiatives of relevance, e.g. EURO-3C, EUCloudEdgeIoT, Next Generation Internet, NGI Commons. Aligning your R&D with these ecosystems allows you to shape the emerging "**Open Internet Stack**" while capturing strategic Horizon Europe funding.

- **Audit your supply chain:** Under the newly enforced **NIS2 Directive** and the **Cyber Resilience Act (CRA)**, organisations are legally responsible for the vulnerabilities of their vendors. Audit sub-processors now and prioritise vendors who can continuously prove a "Clean EU Supply Chain." Crucially, when auditing smaller partners, utilise the forthcoming simplified technical documentation forms (CRA Article 31). By accepting these concise templates, **you enable SMEs to prove compliance without the exhaustive overhead required of large firms**. This directly bolsters strategic autonomy by ensuring local, **small-scale innovators remain viable** in the digital supply chain rather than being forced out by compliance costs.

For Swiss-Based Organisations

While Switzerland sits outside the EU, the "Brussels Effect" makes the Tech Sovereignty Package a direct compliance mandate for Swiss organisations operating across borders.

- **Navigate the FADP vs. CLOUD Act clash:** Switzerland enforces the strict Federal Act on Data Protection (FADP). If a Swiss enterprise uses a US-based hyperscaler, that data is subject to the US CLOUD Act, creating a direct legal conflict. Implementing HYOK with a Swiss-based encryption provider ensures that even if an USA cloud provider is required, they cannot hand over readable Swiss data.

- **Prepare for Extraterritorial Supply Chain Audits:** If your Swiss organisation provides software, IoT devices, or IT services to an EU market, or if you supply an EU critical infrastructure company, you must comply with **NIS2** and the **CRA**. Your EU clients are legally required to audit you, and failing to demonstrate a "Clean Supply Chain" will result in being locked out of EU procurement contracts. **Crucially, for Swiss SMEs, a concrete survival strategy is to proactively utilise the forthcoming simplified technical documentation forms (CRA Article 31).** These concise templates allow you to prove compliance without the massive administrative overhead required of enterprise organisations, ensuring you remain competitively embedded in the EU digital supply chain without being priced out by bureaucracy.

- **Capitalise on Horizon Europe Integration:** With Switzerland's association with Horizon Europe, Swiss researchers and companies can fully participate in and lead European deep-tech consortia. Swiss-headquartered organisations like **Martel Innovate** serve as vital bridges, demonstrating how Swiss entities are successfully coordinating massive EU initiatives. Partnering within these ecosystems is now a direct revenue and R&D pipeline, ensuring Swiss firms remain at the heart of the European Digital Commons.

Concluding Remarks

Navigating the 2026 Tech Sovereignty Package is no longer just a legal compliance exercise: It becomes an essential part of public and private organisations' business strategies.

Clearly, the financial and operational toll of this transition will be substantial. Adapting to this new paradigm requires upfront capital to comprehensively audit complex supply chains for NIS2 and CRA compliance, engineer "sovereign cloud" exit strategies, and absorb the friction of turning away from entrenched, highly subsidised foreign tech stacks. For many IT and compliance departments, this will feel like a costly restructuring of their entire digital foundation.

However, the EU is actively mitigating this friction to ensure local innovators are not left behind. A massive strategic opportunity for smaller organisations lies in the upcoming **single-entry point** for incident and vulnerability reporting. Designed to harmonise the overlapping reporting mandates of the CRA, NIS2, and the GDPR, this one-stop-shop mechanism allows SMEs to notify authorities without drowning in redundant paperwork. By radically reducing the administrative reporting burden, the EU is making the financial transition to "sovereign cloud" infrastructure and "clean supply chains" much more viable for micro-enterprises.

Ultimately, these initial investments diminish in comparison to the cost of inaction. Failing to adapt means risking total exclusion from the massive European public procurement market, facing severe regulatory penalties, and being locked out of critical enterprise supply chains.

Whether you are an EU enterprise adapting to strict new mandates or a Swiss organisation looking to capitalise on the newly reopened Horizon Europe funding windows, the organisations that act today will define the next decade of European digital leadership. The line between regulatory risk and massive strategic opportunity has never been thinner.

MARTEL
innovate

REACH OUT TO US! WE WANT TO HEAR FROM YOU

CONTACT US

info@martel-innovate.com
+ 41 77 415 65 88

Zurich Office | Martel GmbH
Überlandstrasse 111
8600 Dübendorf, Switzerland

Chiasso Office | Martel GmbH
Corso San Gottardo 6a
6830 Chiasso, Switzerland

Amsterdam Office | Martel Innovate B.V.
Keizersgracht 482,
1017EG Amsterdam, The Netherlands