Building the Case: EuroStack

24 November 2025

Written By: *Jesus Gonzalez, Ting-An Li, Rubina Almas, Nicholas Bayer, Sarab Singh Walia, Nadia*

IEF THUNDERBIRD SCHOOL OF GLOBAL MANAGEMENT | ASU Arizona State University

"Securing European tech sovereignty starts with investing in advanced technologies and in making it possible for people to improve their digital competence"

- Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy

We extend our sincere thanks to all the interviewees, sponsors, and mentors whose generous support and insightful contributions made this study possible.

Innovate Europe Foundation
Clark Parsons
IE.F Managing Director

Antonia Wagner
Manager, Policy & Communications

Ecosia
Wolfgang Oels
Chief Operating Officer

Abilian
Stéfane Fermigier
Founder & Chief Executive Officer

Nextcloud
Vanessa Steeg
Team Lead Account Management

IONOS
Mark Neufurth
Enterprise Strategist Public Sector

Safespring
Daniel Melin
Business Development & Strategy

Table of Contents

Executive Summary

The European Union (EU) is currently grappling with substantial challenges related to digital and data sovereignty, primarily due to its considerable reliance on IT infrastructure and cloud solutions from the United States and China. In response, the EU has begun laying the groundwork for a more autonomous technological ecosystem, known as the EuroStack. While this vision holds promise, the path towards technological independence is complicated by persistent stakeholder reluctance to move away from long-established hyperscalers, which are widely viewed as reliable, familiar, and cost-effective.

This white paper addresses these concerns directly. Through a detailed cost analysis, a structured comparison of the US, EU, and in-house IT models, and global benchmarking insights from India and Airbus, we demonstrate that transitioning to EU-based cloud and software alternatives is not only economically viable but strategically advantageous. We show that EU solutions offer competitive pricing, stronger compliance with European regulations, and reduced exposure to geopolitical and legal risks.

The paper concludes with three strategic pillars for advancing digital sovereignty. First, it recommends investing in sovereign cloud infrastructure through coordinated public-private funding and clear communication of long-term cost and value benefits. Second, it emphasizes the need to make cloud adoption user-friendly by prioritizing interoperability, simplifying migration, and offering flexible integration options. Third, it advocates for expanding partnerships through hybrid architectures and shared governance arrangements, drawing lessons from Airbus's successful pan-European collaboration and India's rapid scaling of digital public infrastructure.

Despite these opportunities, the paper acknowledges persistent regulatory hurdles and market fragmentation across EU member states, which complicate harmonization and slow adoption. Early adopters of EuroStack solutions, however, stand to gain significant influence in shaping standards and securing a leadership position in the emerging digital ecosystem. By highlighting the strengths of EU providers and the cost-efficiency of local cloud ecosystems, the paper aims to support a broader shift toward a resilient, interoperable, and sovereign European digital infrastructure.

Problem Statement

European organizations face mounting challenges in balancing cost efficiency, regulatory compliance, and data sovereignty while relying on US-based hyperscalers, which control an estimated 75–80% of the European cloud computing market (Boston Consulting Group, 2025; CERRE, 2024; Wire, 2025). This reliance underscores Europe's vulnerability to regulatory risk and vendor lock-in, and limits local economic value retention (CERRE, 2024; Bria, 2024). While competitive EU-based alternatives exist, adoption remains limited, especially in sectors—public or private—that are historically slow to transition, due to factors including limited awareness, mistrust in newer vendors, and ongoing single market barriers (Wire, 2025; CERRE, 2024).

A comprehensive, European-built cloud infrastructure (Kathuria & Sánchez-Cacicedo, 2025) is seen as central to tackling these challenges (Kathuria & Sánchez-Cacicedo, 2025; European Commission, 2025). EuroStack, when adopted, could meaningfully reduce infrastructure and operational costs, ensure GDPR compliance, and secure long-term value retention for EU businesses (European Commission, 2025; CERRE, 2024). Scenario analyses suggest that if EU organizations transition proactively to EuroStack, they can steadily lower costs and dependency, while late or partial adoption risks cementing US dominance, increasing future risk exposure and regulatory complexity (Kathuria & Sánchez-Cacicedo, 2025; Boston Consulting Group, 2025). Recent momentum—driven by new regulations like the Digital Markets Act and increased scrutiny over cross-border data transfers—has created a stronger incentive for switching providers now, as organizations seek to avoid heightened compliance and reputational risks following high-profile enforcement actions and US policy changes (European Commission, 2025; Bendiek, 2021).

Technology and AI independence have become increasingly crucial for national security, with EU policy leaders and industry experts warning of strategic vulnerabilities if core technology infrastructure—and the emerging field of artificial intelligence—remains under US or Chinese control (Warso, 2025; Bria, 2024; European Movement International, 2021). This concern is reflected in policy debates and official declarations. As of 2025, at least 19 EU member states have published policy statements or official strategies regarding digital sovereignty, aiming to foster greater autonomy and control over critical digital infrastructure (Wire, 2025; European Union, 2022).

Furthermore, at least 17 EU countries have formal policy frameworks or national strategies on artificial intelligence, ranging from ethical guidelines to future-proofing for national security and industrial competitiveness (Wire, 2025; European Round Table for Industry, 2024).

Despite these developments, national implementation remains uneven, and the need for a coordinated approach to technological sovereignty—especially as AI's role in security, economy, and administration grows—has never been more urgent (European Commission, 2025; Warso, 2025). In sum, recent regulatory reforms, digital sovereignty movements, and growing awareness of geopolitical risk have increased the pace at which EU companies are reconsidering their dependence on US hyperscalers and exploring strategic transitions to European-built cloud services (Boston Consulting Group, 2025; CERRE, 2024).

Market Landscape

Role of EU Regulations in Shifting Tech Choice

Europe's recent regulatory reforms have become the driving force behind its transition toward digital sovereignty. The Digital Services Act (DSA), Digital Markets Act (DMA), and Data Act represent a coordinated effort to rebalance power in the digital economy and reduce long-standing dependence on non-European providers. Together, they establish a foundation that protects European values of transparency, fairness, and accountability while promoting a market environment where innovation and sovereignty can coexist.

For decades, Europe's digital infrastructure has relied on foreign hyperscalers such as Amazon, Microsoft, and Google. This dependence exposes European data to external legal frameworks such as the U.S. CLOUD Act and FISA 702, which allow American authorities to access data stored in Europe through U.S.-owned providers. As a result, European companies face compliance uncertainty under the GDPR and rising risks of data misuse. These concerns have led policymakers to view regulation not merely as a constraint but as a strategic tool to strengthen competitiveness, protect citizens, and stimulate homegrown technological growth.

The DSA, fully enforced since 2024, seeks to create a safer and more transparent digital environment. It holds large online platforms accountable for the content they host, demands algorithmic transparency, and introduces uniform rules across all member states. For users, this means greater control and trust in the digital sphere. For European businesses, it simplifies compliance and creates a level playing field across borders. The law also helps restore fairness by curbing the dominance of non-EU platforms that have long benefited from uneven regulation.

The DMA complements this framework by addressing structural inequalities within the digital market. It designates "gatekeepers," meaning companies that control core platform services such as app stores and search engines. By requiring these platforms to open their ecosystems, share user data with business partners, and ensure interoperability, the DMA encourages competition and innovation from smaller European firms. While compliance costs remain high for large foreign actors, the regulation empowers domestic startups to access markets that were previously closed.

The Data Act adds a new dimension by promoting fair access and use of industrial and consumer data. It introduces rules that prevent data hoarding and enable users to transfer data between services without barriers or excessive fees. For small and medium enterprises, this means new opportunities to build data-driven products, strengthen business models, and participate in a more open digital ecosystem. It also supports the European Union's broader objective of creating a single, interconnected data market that operates under European jurisdiction.

Together, these regulations mark a turning point. They encourage companies to choose EU-based cloud solutions such as IONOS, OVHcloud, and Nextcloud, or to invest in in-house systems that guarantee compliance and autonomy. The regulatory shift transforms Europe's technology landscape from one shaped by dependency into one built on trust, accountability, and democratic oversight.

Regulatory challenges

- The European Union's ambition to lead in digital governance comes with significant implementation challenges. Its legal environment, though visionary, remains fragmented and administratively demanding. These complexities slow the pace of adoption for local firms and risk widening the gap between policy intent and market reality.
- The most immediate challenge is fragmentation. Although EU laws aim for harmonization, member states often apply them differently. Variations in taxation, procurement, and data-handling procedures make it difficult for firms to scale across borders. This inconsistency particularly affects small and medium enterprises (SMEs) that lack the capacity to manage multiple compliance systems.
- A second challenge involves regulatory overlap. The DSA, DMA, Data Act, NIS2 Directive, and GDPR each introduce distinct but interlinked requirements. Managing them simultaneously demands technical expertise, continuous monitoring, and dedicated resources. Companies must invest heavily in legal, cybersecurity, and data-governance teams to meet obligations, which can divert funds away from innovation and product development.
- There is also the issue of enforcement asymmetry. Some member states have well-resourced digital authorities, while others lack institutional capacity. Uneven implementation weakens the deterrence effect of regulation and leads to legal uncertainty that discourages long-term investment in sovereign infrastructure.
- Moreover, the pace of legislative change creates regulatory fatigue. Constant updates to AI, cybersecurity, and sustainability rules force firms to adapt rapidly, often without sufficient guidance or technical support. This environment favors large multinationals that can absorb compliance costs, while smaller domestic players struggle to keep up.
- To manage these pressures, many companies are turning to RegTech solutions, centralized compliance playbooks, and partnerships with specialized legal advisors. Some have formed internal teams that integrate legal, IT, and risk functions to ensure consistency across borders. Others engage proactively with EU regulators to clarify interpretations and influence policy design.
- Despite the costs, these regulations lay the groundwork for a more transparent and trustworthy digital market. They strengthen Europe's credibility as a global standard-setter and encourage the development of technology that reflects its social and ethical priorities. Over time, compliance will become not just an obligation but a mark of reliability and a competitive advantage for firms operating within the European framework.

Overview of the Three Models: US Providers, EU Providers, and In-House Infrastructure

Europe's shifting regulatory environment and accelerating push for digital sovereignty have produced three distinct pathways for European businesses seeking secure, compliant, and scalable digital infrastructure. Organizations today choose between (1) US hyperscalers such as AWS, Microsoft Azure, and Google Cloud; (2) EU-native cloud providers such as IONOS and OVHcloud, often paired with sovereign collaboration platforms such as Nextcloud; or (3) fully in-house infrastructure built and operated internally. Each model presents radically different cost structures, regulatory exposure levels, and implications for strategic autonomy. To understand which

model best supports Europe's long-term sovereignty objectives, it is necessary to analyze each one through detailed cost evaluation, risk exposure, and benefit trade-offs. Taken together, these three dimensions create a

complex, multi-layered landscape that shapes decision-making for enterprises, governments, and SMEs across the region.

Context: Why Market Concentration Matters for Europe

Before comparing cloud models, it is useful to understand the environment European organizations operate in. The two figures highlight a simple but important reality:

1. **Cloud Provider Concentration:** As shown in Exhibit A, The global cloud market is dominated by three US hyperscalers–Amazon, Microsoft, and Google—together holding over two-thirds of worldwide IaaS/PaaS revenue. European providers such as OVHcloud, IONOS, and others remain below 5%, making them far less visible and less integrated into enterprise defaults.

2. **Desktop OS Dependency:** As shown in exhibit B, Windows and macOS account for more than 80% of global desktop operating systems, meaning most enterprise environments are already tied into US ecosystems for identity, productivity, and developer tooling.

The following graphs represent how deeply American technology runs through European enterprises. The first graph illustrates why European organizations naturally default to U.S. cloud stacks: the software foundation they rely on is already American, creating a structural dependency long before cost or policy become factors. The second graph highlights the operating systems most commonly used within EU organizations, further reinforcing the extent of American technological dominance at the foundational level.

Exhibit A

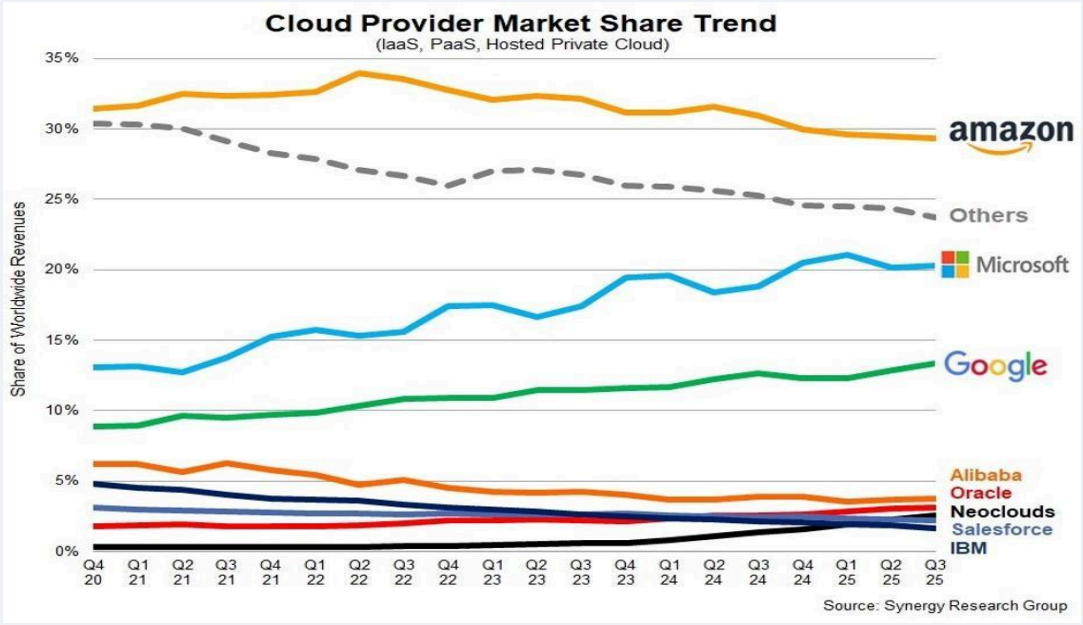
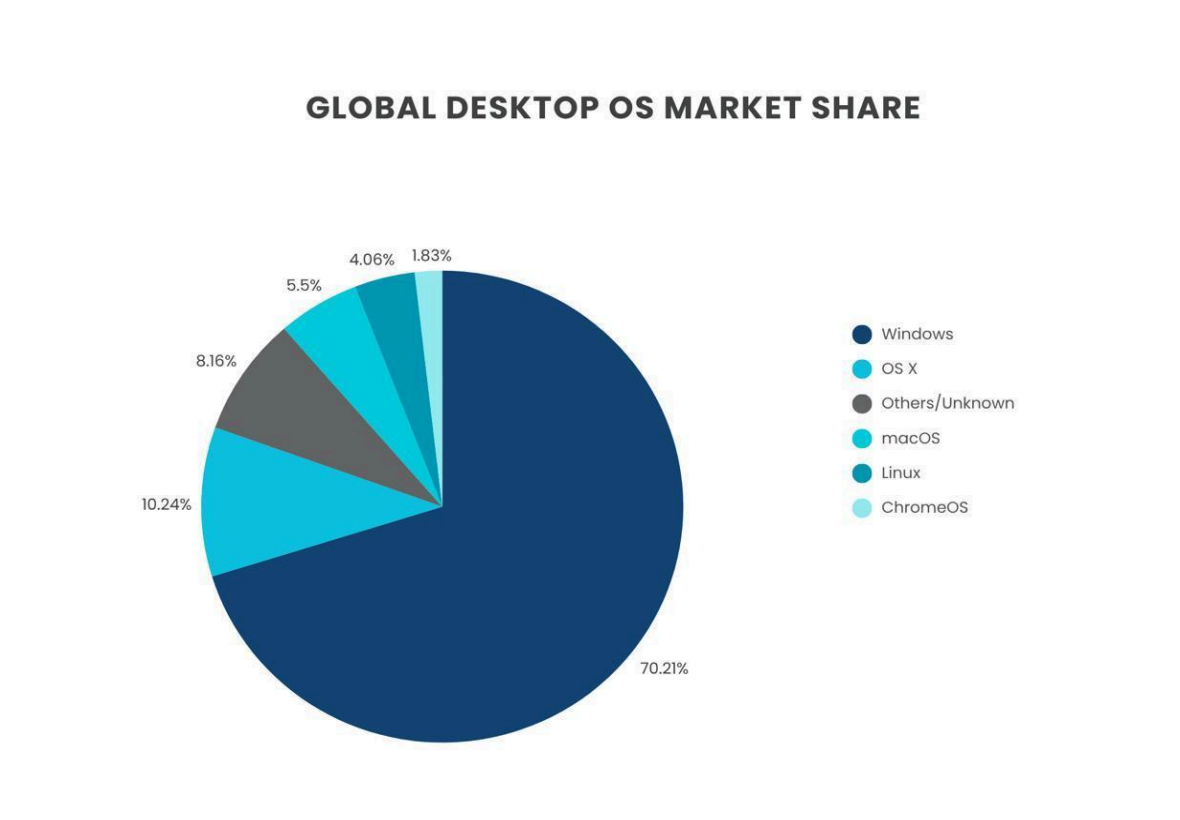


Exhibit B



Cost Analysis

The cost analysis compares the full annual cost of cloud and IT operations across US hyperscalers, EU-native cloud providers, and internally built IT departments. The calculations below use the same baseline workload for fairness:

Here is the Baseline Workload Assumption:

- 10 VMs (8 vCPU, 32 GB RAM) running 24/7
- 2 TB block storage + 1 TB object storage
- 5 TB monthly outbound data
- 1 load balancer + 10 public IPs
- 1,000 users (SMB scale)
- This baseline mirrors a mid-sized EU enterprise operating core business applications such as CRM, ERP, collaboration systems, and document storage.

Cost Structure of US Providers (AWS, Microsoft Azure, Google Cloud)

US hyperscalers maintain the world's most extensive and advanced cloud platforms, but this capability comes at a significantly higher price point for European organizations. Based on pricing from the Frankfurt and Germany West Central regions, annual infrastructure costs for a 10-VM workload range from €38,000 (AWS) to €132,800 (Azure) to €63,000 (Google Cloud) before software licensing and collaboration tools are added.

AWS Annual Cost Breakdown:

The following values come directly from AWS Frankfurt-region pricing (EC2 t3.2xlarge + gp3 storage + S3 + Network egress):

- Compute[1]: €29,784/year
- Block Storage[2] (2 TB): €2,160
- Object Storage[3] (1 TB): €276
- Data Transfer[4] (60 TB/year): €5,100
- Load balancer[5]: €245
- Elastic IPs[6]: €438

Total AWS Infrastructure Cost: ≈ €38,000/year

However, infrastructure alone is not enough. European SMBs typically use Microsoft Office 365 E5 for productivity and security. Combining AWS infrastructure with Microsoft E5 and Windows licensing raises the per-user cost to €648.97 per user per year, resulting in:

Total annual AWS-based operating cost (1,000 users): €648,970

For a small business with at least 100,000 users, the rough estimate is:

€648.97 × 100,000 = ≈ €64.9 million per year.

Microsoft Azure Annual Cost Breakdown[7]:

Costs were calculated using Azure's Germany West Central region pricing:

- Compute[8]: €125,000/year
- Block Storage[9] (2 TB): €2,160
- Object Storage[10] (1 TB): €276
- Data Transfer[11]: €4,700
- Load balancer[12]: €245
- Public IPs[13]: €438

Total Azure Infrastructure Cost: ≈ €132,800/year

Adding Microsoft 365 E3[14] (commonly used by EU firms) at €420/user/year produces:

Azure total annual cost (1,000 users): ≈ €132.8k infrastructure + €420k licensing ≈ €552,800

For a European small business with 100,000 users, the estimated Azure + Microsoft 365 E3 annual operating cost is €55.3 million per year

Google Cloud Annual Cost Breakdown:

Using Europe-region GCP pricing:

- Compute[15] (10 × n2-standard-8 type): ≈ €57,000/year
- Block Storage[16]: €2,160
- Object Storage[17]: €276
- Data Transfer[18]: €4,600

Total GCP Infrastructure: ≈ €63,000/year

- Adding Office 365 E3 subscriptions:

Google Cloud annual cost (1,000 users): €63k + €474k + €136k = ≈ €673,970

For a European small business with 100,000 users, the estimated Google Cloud + Microsoft Office 365 E5 annual operating cost is ≈ €67.4 million per year

Summary Cost Profile: US Hyperscalers

Despite some variability in compute rates, all three US providers converge on a similar cost range once EU companies account for licensing, productivity suites, and security:

AWS: €64.9 million per year.
Azure: €55.3 million per year.
Google Cloud: €67.4 million per year

This places US hyperscaler pricing firmly between €553–€674 per user per year, making them the middle option for expenses in this comparison.

Cost Structure of EU Providers (IONOS, OVHcloud + Nextcloud)

EU-native providers offer dedicated data residency, simpler pricing models, and lower infrastructure overhead. Costs for equivalent workloads are dramatically lower — often 4–5× less than US hyperscalers.

IONOS + Nextcloud Cost Breakdown

Because IONOS offers only IaaS and PaaS, sovereign SaaS functionality (documents, calendars, sharing) requires Nextcloud Enterprise on top.

IONOS Infrastructure Costs[19]

Using IONOS pricing for 8 vCPU / 32 GB RAM VMs (€0.162/hr):

Compute: €14,191/year
Block Storage (2 TB): €1,776
Object Storage (1 TB): €59
Outbound data (after free 2 TB/month): €2,160
Load balancer: €193
Public IPs: €720

Total IONOS Infrastructure: ≈ €19,100/year

Nextcloud Enterprise Licensing[20]

100 users × €3/user/month = €3,600/year

Scaled to 1,000 users, enterprise pricing remains linear, but the combined stack requires:

Ubuntu Pro Support (EU-grade security compliance)[21]

Approx. €150/user/year = €150,000/year for 1,000 users
(Sourced from Ubuntu Pro enterprise support tiers)

Final Combined Annual Cost

Base infra + NC + OS = €19,100 + €3,600 + €150,000

Add 50% markup for OPEX + R&D + margin (standard for MSPs)

This produces a per-user price:

≈ €36/user/year

and an annual total:

≈ €205,100/year for 1,000 users, including OPEX, Nextcloud, and Ubuntu Pro compliance.

Now scale to 100,000 users

100,000 × €205.10 = €20,510,000 per year

IONOS + Nextcloud annual cost for 100,000 users ≈ €20.5 million

OVH cloud Cost Breakdown[22]

OVHcloud is Europe's most cost-efficient sovereign cloud provider. Using raw workload calculations:

Compute: €9,723/year
Block Storage: €960
Object Storage: €85
Egress: €600
Network + IPs: €320

Total OVHcloud Infrastructure: €11,700/year

After 50% operational markup:

Final OVH cloud per-user cost: ≈ €17.50/user/year
Total cost for 1,000 users: €168,000/year

Now scale to 100,000 users

100,000 × €168 = €16,800,000 per year
OVHcloud annual cost for 100,000 users ≈ €16.8 million

Summary Cost Profile: EU Providers

IONOS + Nextcloud: ≈ €20.5M/year
OVHcloud: ≈ €16.8M/year

EU cloud providers are 3–5× cheaper than US hyperscalers, particularly because (1) storage and egress rates are dramatically lower, and (2) European providers offer better cost predictability with fewer pricing changes.

Cost Structure of In-House IT Departments (Germany and France)

In-house infrastructure is the most expensive option due to personnel-heavy operational requirements.

Germany Annual Costs[23]

Salary Costs:

CTO: €135,000
3 Senior Engineers: €270,000
5 Mid-Level Engineers: €325,000
2 DevOps Engineers: €150,000

Total Salaries: €880,000/year

Infrastructure CAPEX[24] (year 1):

Servers, networking, migration: €200k–€500k

Ongoing OPEX:

Maintenance, bandwidth, cooling, licenses: €100k–€300k
Total Year 1 Cost: €1.1–€1.5M
Year 2+ Cost: €900k–€1.1M
Cost per user (1,000 users): €900–€1,100/user/year

Scale to 100,000 users[25]:

100,000 × €900 = €90,000,000/year
100,000 × €1,100 = €110,000,000/year

Germany In-House IT Annual Cost for 100,000 Users:

≈ €90M – €110M per year

France Annual Costs[26]

Total Salaries: €765,000
Year 1 Total: €1.0–€1.3M
Year 2+: €800k–€1.0M
Per-user cost: €800–€1,000/year

Scale to 100,000 users

100,000 × €800 = €80,000,000/year
100,000 × €1,000 = €100,000,000/year

France In-House IT Annual Cost for 100,000 Users:

≈ €80M – €100M per year

Summary In-House Cost Profile:

In-house infrastructure remains the most expensive model, costing up to 10× more than EU cloud options.

Risk Assessment

US Hyperscalers

US-based cloud providers bring powerful infrastructure and ecosystem benefits, but they carry significant legal and operational risks from a European sovereignty standpoint. The CLOUD Act creates potential exposure of European data to U.S. authorities, even if it is stored in European data centers. This can undermine trust in data control. There is also substantial vendor lock-in: once an enterprise embeds its workflows and data into AWS, Azure, or Google Cloud, migrating becomes technically costly, time-consuming, and risky. Additionally, aggressive pricing change behavior — such as AWS's frequent pricing updates — complicates budgeting and financial forecasting. For sovereign or highly regulated entities, these risks can outweigh raw performance advantages.

EU Providers

European-native providers such as IONOS and OVHcloud reduce regulatory exposure because their operations are fully governed within the EU, respecting GDPR and related local laws. Because they prioritize data residency and compliance, they avoid many of the legal risks faced by hyperscalers. However, they face their own challenges: their service portfolios are less mature, especially in advanced cloud-native AI or analytics features. There is also fragmentation across EU providers, making cross-border scaling and standardized procurement difficult. Furthermore, clients may face price volatility or surprise cost increases (for example, IONOS's renewal rates or license upsells), and migrating away from one EU provider to another can also create lock-in, albeit less extreme than with US providers.

In-House

An in-house model maximizes control over data, infrastructure, and policies, but places full operational burden on the organization. Staff must be highly skilled, security must be maintained internally, and teams need to keep up with compliance (e.g., GDPR, NIS2, AI Act). There is also risk in scale: cost efficiencies depend heavily on size and usage. If the business or user base does not scale as planned, the cost per user may remain high. Technical risks, such as managing legacy systems or migrating older data, also pose real challenges. Furthermore, time lost during migration, training, systems integration, and workflow redesign can undermine productivity in the near term, and financial risk can rise if initial cost estimates were too optimistic.

Benefits & Drawbacks Comparison

US Hyperscalers

The most compelling advantage of US hyperscalers is their unmatched scale, global infrastructure, and rich service global reach, and extensive third-party ecosystems. However, these advantages come at the price of sovereignty lock-in that makes transitions away from these platforms difficult.

EU Providers

European providers like IONOS paired with Nextcloud or infrastructure-only providers such as OVHcloud offer a powerful blend of regulatory alignment, cost predictability, and data residency. Their models deliver much lower per-user costs in sovereign deployments than hyperscalers. On the downside, these services may lack the broader service breadth of US clouds and some advanced features, meaning highly specialized or cutting-edge workloads may not yet find all needed tools in EU-native stacks.

In-House

Maintaining your own IT infrastructure offers full operational sovereignty– you control access, updates, security, and architecture. Licensing costs are minimized if open-source software is used, and there is no reliance on third-party platforms. That said, this model demands substantial upfront investment, ongoing personnel costs, and operational burden. It also implies risk: any failure in internal security or architecture translates directly into business risk, and scalability might be slower and more resource-intensive.

Soft Barriers Between EU Countries

Even though European cloud providers present a strong cost and compliance case, non-technical barriers slow adoption across borders. Many enterprises and public institutions are accustomed to working with national or regional vendors, shaped by procurement traditions and long-standing contracts.
Language, trust, and differing regulatory interpretations can discourage cross-border provider selection. In addition, procurement frameworks and tenders remain fragmented, reflecting national rather than EU-wide standards, which limits economies of scale and unified adoption.

Winners vs. Losers

If EU organizations increasingly purchase cloud services from providers based in other member states, the winners are likely to be the sovereign providers themselves — firms like IONOS and OVHcloud, which can scale across borders and benefit from broader demand. Public sector organizations and SMBs stand to gain from lower-cost, high-compliance solutions. On the other hand, losers may include incumbent US hyperscaler vendors (losing market share), smaller local hosting companies without a pan-European presence, and countries whose local cloud firms cannot compete in cost or compliance with cross-border EU providers.

Over time, greater cross-border EU cloud adoption could reshape Europe's digital ecosystem, but only if procurement, trust, and regulatory harmonization improve in parallel with cost optimization.

Global Benchmark

To inform the EU's strategy for competing with US technology firms, two benchmark cases were analyzed. The first is Airbus, a notable example of successful EU competition with US companies. The second is India's technology sector, which has demonstrated robust growth and increasing competitiveness with US firms. While not all elements of these examples are directly applicable and some approaches should be avoided they provide valuable context for the EU as it formulates its own competitive strategy.

Airbus as a historical reference

In the 1970s, when European countries depended almost entirely on American companies like Boeing for aircraft, it became too expensive and too risky to manufacture planes, for any one country or company, in isolation.

The solution: France, Germany, Spain, and the UK formed Airbus as a European, state-owned joint project. The governments could share the high costs through repayable loans and joint research programs. This allowed Airbus to design, build, and market competitive aircraft. By this means, Europe was able to keep cutting-edge technology, produce thousands of skilled jobs, and ultimately create a world leader known as Airbus. The model also proved that when Europe shares risks and resources, it would be a lot less dependent and would be able to build global industrial strength.

The same approach leads us to the EuroStack. Building a digital cloud, creating an infrastructure requires lots of investment, long lead times, and coordination. EuroStack can operate on shared-risk funding, either repayable new innovation loans or European infrastructure funds, to help local techs improve. Working together under shared standards and certifications, such as the European Cloud Services Scheme (EUCS), will help create a single European digital market. Beyond all that, there is also a classic early demand that such a "Buy European Cloud" policy can easily generate, just as European airlines once bought into Airbus in support of that venture. Further public investment in research, open-source software, AI, and cybersecurity has also strengthened the digital ecosystem, but only under transparent and fair support under EU regulations.

Airbus shows that Europe can turn dependency into leadership when it pools resources, shares risk, and invests with purpose.

What Aspects of the Airbus Case Could Work for Tech (EuroStack)

Pan-European Collaboration: Airbus successfully unified diverse national industrial resources to overcome fragmentation within Europe. EuroStack can apply this approach by bringing together leading EU cloud and AI companies to advance a shared commitment to technological sovereignty.

Public–Private Partnership: Airbus had the benefit of public money. For its development, the EuroStack should get public-private partnership funding from the EU and encourage investments with national programs for infrastructure and adoption.

Standardization and Interoperability: Airbus relied on common standards; EuroStack should ensure the priority of interoperability among software and data platforms of the EU in order to have any chance to compete with US hyperscalers.

Long-Term Strategic Vision: The success of Airbus was decades in the making. EuroStack needs a patient and strategic approach, equally long-term.

Strong European Branding: Airbus, recognized as a leading industrial force in the EU, positions itself as Europe's trusted "sovereign cloud" provider and is a prime candidate for EuroStack.

What Aspects Won't Work (What to Avoid)

Protectionism Over Competitiveness: EuroStack has to compete in terms of quality, innovation, and interoperability, not only by favoring regulation.

Political Fragmentation: Initial Airbus deficiencies were due to national jealousies; thus, EuroStack governance should be engaging and clear.

Ignoring Market Incentives: Unlike the aircraft industry, tech markets change rapidly, and the EuroStack must be responsive to user needs and market feedback.

Why India Was Chosen as a Case Study

India represents one of the most successful examples of a country rapidly scaling its digital economy in a relatively short period, while simultaneously reducing dependence on foreign technology firms. Unlike other benchmarks, India’s model is unique in the way it combines public digital infrastructure, massive skills development, and a thriving private ecosystem to create competitive capacity at global scale.

For the EU, which is exploring ways to strengthen technological sovereignty, India offers not a direct blueprint but a set of strategic levers: the use of digital public goods, demand creation through government-led platforms, and talent development at national scale. India’s experience provides insight into how systemic, infrastructure-first approaches can catalyze private innovation, an outcome that aligns closely with Europe’s ambitions for EuroStack.

Overview of India’s Tech Landscape

Over the last decade, India has shifted from being primarily an outsourcing hub to a global technology powerhouse. This transformation rests on five pillars:

A rapidly expanding Digital Public Infrastructure (DPI): India Stack that comprises Aadhaar (identity), UPI (payments), DigiLocker (data-sharing), and other open APIs–provides the foundational rails on which both

government and private innovation run. These platforms handle billions of transactions monthly and drastically lower the cost of digital service delivery.

A deep talent pool at scale: With millions of engineers graduating annually and strong English proficiency, India has become the world's leading destination for Global Capability Centres (GCCs). Multinational firms from the US and EU rely on Indian engineering teams for R&D, cloud, AI, cybersecurity, and enterprise software development.

Proactive policy support and incentives: State-level subsidies, special economic zones, GCC-friendly policies, and skills development programs have accelerated investment. Cities like Bengaluru, Hyderabad, and Pune now function as global engineering hubs.

A thriving services and export economy: India's IT services, BPO, and engineering R&D sectors generate more than $250 billion annually, with strong export orientation. Scale in services has reinvested into tech product development, fintech, and SaaS.

A maturing startup ecosystem: Incubation programs, venture capital growth, and policy support (e.g., Startup India) have created more than 100 unicorns. Even after VC slowdowns, India continues to produce digital-first companies with global reach.

This combination of public infrastructure + private innovation is what makes India uniquely relevant to Europe's digital sovereignty ambitions.

What Has Been Working for India

India's success stems from systemic levers that create *both supply and demand* for technology simultaneously.

Large-scale public digital infrastructure (India Stack): The single most important catalyst for India's digital rise is its DPI. Aadhaar created universal digital identity; UPI created cashless payments rails; DigiLocker enabled secure data exchange. These infrastructure layers dramatically lowered onboarding costs, automated compliance, and enabled frictionless citizen services. Most importantly, they allowed private companies to innovate on top of government-created rails, producing massive network effects.

Abundant engineering talent at globally competitive cost: Because wages, living costs, and social protections are lower, India enjoys a price advantage. This cost structure enabled the rapid proliferation of GCCs and service exports, giving India an extraordinary scale advantage. The volume of engineers allowed companies to grow quickly, take on global projects, and support continuous 24/7 development cycles.

Targeted public incentives and industry clustering: Indian states aggressively competed to attract tech investment, offering tax breaks, subsidies, infrastructure, and dedicated tech parks. These incentives helped create world-class clusters such as Bengaluru and Hyderabad, accelerating innovation cycles.

A large and growing digital consumer base: With over 800 million internet users, India's domestic market creates natural demand for digital services, giving companies a huge testbed for scaling products.

A supportive startup and VC environment: India's funding boom over the past decade allowed fast experimentation, helping startups grow into global challengers, particularly in fintech, SaaS, education, and logistics.

These conditions, public infrastructure, talent, incentives, scale, and startups– together produce a powerful ecosystem that has allowed India to compete with US firms in cost-sensitive and innovation-driven sectors.

Why the EU Cannot Directly "Copy" India

Despite the value of India's model, Europe faces structural differences that make a direct replication impossible.

Regulation and privacy constraints: Europe operates under GDPR, ePrivacy, and strict procurement transparency rules. India's DPI model, while effective, is far more centralized and permissive. A European equivalent must be built with privacy-by-design and distributed governance.

Higher labor costs and social protections: Europe cannot replicate India's low-cost, high-volume engineering workforce. This eliminates the outsourcing-led model that powered India's growth. Europe must instead pursue a strategy based on quality, specialization, and interoperability, not labor arbitrage.

Political Fragmentation and Lack of a Unified Digital Market: India is a single country with central authority over digital infrastructure. The EU consists of 27 states with different political priorities, procurement rules, and digital readiness levels. Creating a unified digital infrastructure requires more coordination and negotiation.

Different public expectations around state-led technology: European societies demand high transparency, accountability, and strong data protection. Aadhaar-style centralized platforms may face public scrutiny or legal challenges.

Capital Market Limitations: Europe lacks the scale and aggressiveness of India's VC cycle. This means that innovation and scaling must rely more on public-private partnership and less on rapid private funding.

For these reasons, the EU must adapt and not replicate India's strategy.

What the EU Can Adopt From India and Why It Would Work

India's rapid digital transformation offers several lessons that the EU can adapt without compromising its regulatory values or privacy standards. While Europe cannot copy India's low-cost labor model or its centralized political system, three elements of India's digital strategy translate directly into the European context and strongly support the development of EuroStack.

The first is the concept of Digital Public Infrastructure. India Stack demonstrates how a shared set of open, public digital rails can unlock innovation at scale. Systems such as UPI for payments and DigiLocker for data exchange work because they provide standard, government-backed APIs that any public or private actor can build on. Europe faces fragmentation across national systems for identity, payments, and data sharing. A European Public Infrastructure would not replace what already exists but instead *connect these systems* under a shared, interoperable architecture. This would reduce friction, enable cross-border services, and provide a technical

foundation for digital sovereignty. It would also accelerate adoption of EuroStack by guaranteeing a baseline demand similar to how UPI supported India's fintech growth.

The second transferable element is India's open-source procurement and local innovation policy. India has long prioritized open-source solutions in public sector IT, which reduced licensing costs, increased transparency, and fostered domestic capacity. The EU has strong alignment with this approach, as open-source technologies offer

auditable code, reduced vendor lock-in, and better compliance with European data protection rules. Encouraging adoption of European open-source platforms such as Nextcloud, Sferical, OVHcloud, SUSE, or EuroLinux would retain economic value within the EU and strengthen the local cloud ecosystem. This also supports workforce development, as open-source communities drive skill growth and R&D.

A third lesson is the centrality of open standards. India's digital infrastructure works because different public and private systems can plug into shared APIs. Europe can adopt the same principle by ensuring that cloud, storage, and data services built under EuroStack follow open, interoperable standards. This reduces switching costs, prevents dominance by any single provider, and allows SMEs to compete with larger players. Interoperability is one of Europe's strongest policy levers, and applying it consistently across EuroStack would encourage competition while maintaining sovereignty.

Together, these three India-inspired mechanisms provide a realistic, sovereignty-aligned path for the EU to strengthen its digital ecosystem. They help overcome fragmentation, stimulate innovation, and reduce dependency on non-European cloud providers while remaining fully compatible with European legal and social norms.

Implementation

Implementing these India-inspired elements in Europe requires a phased approach that fits EU realities: regulatory complexity, multi-country coordination, and strong privacy standards. The goal is not to recreate India's model, but to adapt its most successful mechanisms into a European framework that reinforces EuroStack.

The first step is building a European Public Infrastructure that connects existing national systems into a single interoperable layer. This involves creating common technical standards for payments, data-sharing, and digital services that all EU member states and private actors can adopt. A shared set of APIs would allow public services, banks, healthcare providers, and businesses to operate seamlessly across borders. In practice, this means establishing a core European digital layer similar to India's foundational APIs, but designed around GDPR and EU governance. This layer would serve as the "digital backbone" for EuroStack, ensuring that data flows, service access, and compliance requirements operate consistently across the EU.

The second step is formalizing open-source procurement and innovation incentives. The EU and member states can adopt procurement guidelines that prioritize open-source solutions where feasible, especially in cloud, storage, communication, and collaboration tools. Public sector migration to EU-based open-source technologies would create predictable demand, reduce licensing dependency, and keep investment within Europe. This can be supported by financial mechanisms such as Horizon Europe grants, innovation loans, and targeted tax incentives for companies that develop or maintain European open-source infrastructure. Universities and SMEs should be included as co-developers to ensure talent creation and continuous innovation.

The third implementation step is establishing open standards as a requirement for EuroStack. Standardizing APIs, security requirements, data formats, and interoperability rules ensures that all EU cloud providers can compete on

quality rather than exclusivity. It also prevents vendor lock-in, empowers SMEs, and enables the multi-provider cloud model Europe prefers. A standards-first approach supports seamless cross-border services while maintaining national flexibility and regulatory compliance.

Taken together, these three steps provide a practical roadmap for the EU. They focus on what India does best—shared digital infrastructure, open-source driven innovation, and interoperable standards–while adapting them to Europe's unique institutional landscape. This supports the development of a resilient, sovereign EuroStack that is capable of competing globally and reducing long-term dependence on foreign cloud providers.

Currently, European companies operate with a very high dependence on US hyperscalers, creating significant operational, regulatory, and strategic exposure. With nearly 90% of core digital services running on Microsoft, Amazon, and Google infrastructure, European businesses face rising compliance costs, unpredictable policy risks, and limited control over their own data.

The EuroStack offers a practical path to reduce these pressures while strengthening long-term competitiveness. By shifting progressively toward EU-based cloud and software providers, companies can lower total cost of ownership, simplify GDPR and NIS2 compliance, and decrease the risk of service disruption caused by foreign regulatory changes. Many EU alternatives are already cost-advantaged and designed natively around Europe's data protection environment, reducing both direct expenses and hidden compliance overhead.

Transitioning away from established hyperscalers requires planning and investment, but the business case is increasingly clear: greater control, reduced legal exposure, improved price stability, and a more resilient supply chain for digital services. Early adopters will also benefit from influencing EuroStack standards, opening opportunities for collaboration, preferred procurement, and leadership within Europe's emerging digital ecosystem.

The EuroStack is not only a strategic initiative for governments, it is also a long-term value opportunity for European companies. By investing now in EU-native cloud solutions, businesses can protect their operations, reduce risk, and ensure that their digital infrastructure supports sustainable growth in an increasingly regulated and competitive global market.

Recommendations

Pillar 1: Investment in Sovereign Cloud

- Reduce Long-Term Total Cost of Ownership by Transitioning to EU Cloud Providers
- Strengthen Regulatory Compliance and Reduce Legal Exposure
- Strategic Imperative: Europe's "Airbus Moment" in Digital Infrastructure
- Deepen Public–Private Investment in Digital Infrastructure
- Utilize Targeted Public Funding to Accelerate EuroStack Development
- Improve Cost and Value Communication for Corporate Adoption

Together, these actions focus on moving workloads and data to GDPR-native EU providers, treating cloud and data as strategic assets, and supporting this shift with coordinated public–private investment and clear communication of long-term costs and benefits.

Pillar 2: Make the Cloud User-Friendly

- Enable Frictionless User Transition Through Familiar Design
- Prioritize Interoperability and Simplified Migration
- Assess the Viability of an All-in-One EuroStack Solution
- Promote Customization and Adaptive Integration Across EU Systems

These recommendations aim to make EuroStack easy to adopt by using familiar interfaces, simplifying migration from non-EU providers, and offering flexible, customizable solutions that fit smoothly into existing enterprise environments.

Pillar 3: Partnerships

- Implement a Hybrid EuroStack Architecture to Minimize Fragmentation
- Develop Strategic Long-Term Partnerships With EU Providers
- Encourage Corporate Participation in EuroStack Governance
- Expand Partnerships and EU Ecosystem Coordination

This pillar highlights the need for strong technical and strategic partnerships—combining hybrid architectures, long-term vendor relationships, shared governance, and EU-wide coordination to build a resilient, interoperable EuroStack ecosystem.

References:

Airbus. (2025, November). About us. https://www.airbus.com/en/about-us

Amazon Web Services. (2025). Amazon EC2 T3 instances. AWS. https://aws.amazon.com/ec2/instance-types/t3/

Amazon Web Services. (2025). Amazon EBS pricing. AWS. https://aws.amazon.com/ebs/pricing/?nc1=h_ls

Amazon Web Services. (2025). Amazon S3 pricing. AWS. https://aws.amazon.com/s3/pricing/

Amazon Web Services. (2025). AWS Transit Gateway pricing. AWS. https://aws.amazon.com/transit-gateway/pricing/

Amazon Web Services. (2025). Elastic Load Balancing pricing. AWS. https://aws.amazon.com/elasticloadbalancing/pricing/?nc=sn&loc=3

Amazon Web Services. (2024, February 20). Identify and optimize public IPv4 address usage on AWS. AWS. https://aws.amazon.com/blogs/networking-and-content-delivery/identify-and-optimize-public-ipv4-address-usage-on-aws/

Amundsen Davis. (2023, October 16). Is my U.S.-based company subject to the GDPR? Clearing up European data privacy law misinformation. https://www.amundsendavislaw.com

Bendiek, A. (2021). The impact of the Digital Service Act (DSA) and Digital Markets Act (DMA) on European integration policy. SWP Working Paper Research Division EU/Europe, WP NR. 02. https://www.swp-berlin.org

Boston Consulting Group. (2025, October 30). Cloud cover: Price, sovereignty demands, and waste. https://www.bcg.com/publications/2025/cloud-cover-price-sovereignty-demands-waste

Bria, F. (2024, January 18). European alternatives beyond Silicon Valley: Reclaiming Europe's digital sovereignty. Noema Magazine. https://www.noemamag.com/reclaiming-europes-digital-sovereignty/

Brussels Signal. (2025, July 16). Digital vassals? French government 'exposes citizens' data to US. https://brusselssignal.eu/2025/07/digital-vassals-french-government-exposes-citizens-data-to-us/

CERRE. (2024, February). Competition and regulation of cloud computing services: Economic analysis and review of EU policies. CERRE Report. **https://cerre.eu/wp-content**

Czerniawski, M., & Svantesson, D. (2025). Challenges to the extraterritorial enforcement of data privacy law – EU case study. In Data Privacy Law (pp. 127–142). **https://dataskyddet.se**

Data.europa.eu. (2022, October 4). Data sovereignty in the Digital Decade. **https://data.europa.eu**

Dittrich, P.-J. (2017). Balancing ambition and pragmatism for the Digital Single Market. Jacques Delors Institut–Berlin Policy Paper 204. **https://www.delorscentre.eu**

European Commission. (2025, October). Cloud Sovereignty Framework (Version 1.2.1). Directorate-General for Digital Services. **https://commission.europa.eu**

European Commission. (2016, April). Measuring the economic impact of cloud computing in Europe. **https://digital-strategy.ec.europa.eu**

European Commission. (2025, November). *About the Digital Markets Act.* **digital-markets-act.ec.europa.eu**

European Commission. (2025, November). The Digital Services Act package: Shaping Europe's digital future. **https://digital-strategy.ec.europa.eu**

European Commission, Joint Research Centre. (2024). Data sovereignty for local governments: Considerations and insights. **https://publications.jrc.ec.europa.eu**

European Movement International. (2021, November). Digital sovereignty and citizens' rights. European Movement. **https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/**

European Round Table for Industry (ERT). (2024, March 8). Single Market – Compendium of obstacles. ERT Report. **https://ert.eu**

EU4Digital. (2025, April 9). New step towards the Digital Decade: 2030 policy programme comes into force. **https://eufordigital.eu**

GDPR.eu. (2025, November). General Data Protection Regulation (GDPR) compliance and overview. **https://gdpr.eu/**

GDPR.eu. (2025, November). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

GDPR-info.eu. (2025, November). General Data Protection Regulation (GDPR) – Legal text. https://gdpr-info.eu/

Google Cloud. (2025). VM instance pricing. Google. https://cloud.google.com/compute/vm-instance-pricing

Google Cloud. (2025). Disk and image pricing. Google. https://cloud.google.com/compute/disks-image-pricing

Google Cloud. (2025). Cloud Storage pricing. Google. https://cloud.google.com/storage/pricing

Google Cloud. (2025). VPC network pricing. Google. https://cloud.google.com/vpc/network-pricing

IONOS Group. (2025, November). Reports. https://www.ionos-group.com

Kathuria, R., & Sánchez-Cacicedo, A. (2025, May). Tapping into the momentum: The EU-India Trade and Technology Council — highlights India Stack lessons for EuroStack. Heinrich Böll Stiftung Policy Brief. https://www.boell.de

KPMG. (2024, December). Exploring India's dynamic start-up ecosystem. KPMG International Report. https://assets.kpmg.com

Latham & Watkins LLP. (2023). India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison [Whitepaper]. https://www.lw.com

[6]**Microsoft. (2025).** *Azure Blob Storage – Preise [Azure Blob Storage – Pricing]*. Microsoft Azure. https://azure.microsoft.com/de-de/pricing/details/storage/blobs/

[2]**Microsoft. (2025).** Bandbreite – Preise. Azure. https://azure.microsoft.com/de-de/pricing/details/bandwidth/

[5]**Microsoft. (2025).** IP Addresses pricing. Microsoft Azure. https://azure.microsoft.com/en-us/pricing/details/ip-addresses/

[4]**Microsoft. (2025).** Load Balancer pricing. Microsoft Azure. https://azure.microsoft.com/en-us/pricing/details/load-balancer/

[1]**Microsoft. (2025).** Übersicht über die Preise von Azure [Azure pricing overview]. Microsoft Azure. https://azure.microsoft.com/de-de/pricing/

[3]**Microsoft. (2025).** *Virtuelle Windows-Computer – Preise [Virtual Windows Machines – Pricing]*. Microsoft Azure. https://azure.microsoft.com/de-de/pricing/details/virtual-machines/windows/

Microsoft. (2025). Microsoft 365 enterprise plans and pricing. Microsoft. **https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-plans-and-pricing**

Polish Presidency of the Council of the European Union. (2025, June 16). Data protection: Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens. **https://polish-presidency.consilium.europa.eu**

Sternfels, B., Dhawan, R., Gupta, S., Ganguly, S., & Shah, J. (2025, April). India: The promise and possibilities for global companies. McKinsey & Company. **https://www.mckinsey.com**

Tims, A. (2024, February 8). Ulez fines scandal: Italian police 'illegally accessed' thousands of EU drivers' data. The Guardian. **https://www.theguardian.com**

Usercentrics. (2024, May 31). Digital Markets Act uncovered: Top 30 DMA questions answered. **https://usercentrics.com/knowledge-hub/digital-markets-act-faq-top-30-questions-answered/**

Warso, Z. (2025, October 17). Building digital sovereignty: What does Europe need and how to achieve it. Tech Policy Press. **https://www.techpolicy.press**

Warwick, M. (2025, May 29). Europe eyes digital sovereignty sans big tech. TelecomTV. **https://www.telecomtv.com**

Wire. (2025, October 6). Digital sovereignty in 2025: Why it matters for European enterprises. **https://wire.com/en/blog/digital-sovereignty-2025-europe-enterprises**

Wire. (2025, October 9). The state of digital sovereignty in Europe: Survey insights and strategies for EU-native tech. Wire.com. **https://wire.com/en/blog/state-digital-sovereignty-europe**

Our greatest glory is not in never failing, but in rising every time we fail.

- Confucius