European Digital Dependencies

Diagnosis and Priorities for Public Sector Decision-Makers

Nicolas Roux March 2026

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

European Digital Dependencies. Diagnosis and Priorities for Public Sector Decision-Makers
Nicolas Roux, roux.nse@proton.me, First edition, March 2026.
DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Executive Summary - Senior Policymakers

European public institutions operate on digital infrastructure whose availability, jurisdiction, and governance are determined outside European legal control. This exposure is concentrated in eight technological layers. For six of those eight, production-ready European alternatives exist today. Organisations in Germany, France, and the Netherlands have completed migrations within standard budget cycles, with documented cost reductions ranging from 30 to 50 percent.

The political window for acting on this exposure has not been this favourable in a decade: alignment between documented feasibility, available European providers, and Commission policy momentum. The decisions that activate it are identified in this report, and most are within reach of current institutional authority.

The table below maps the principal European-level instruments to their decision points.

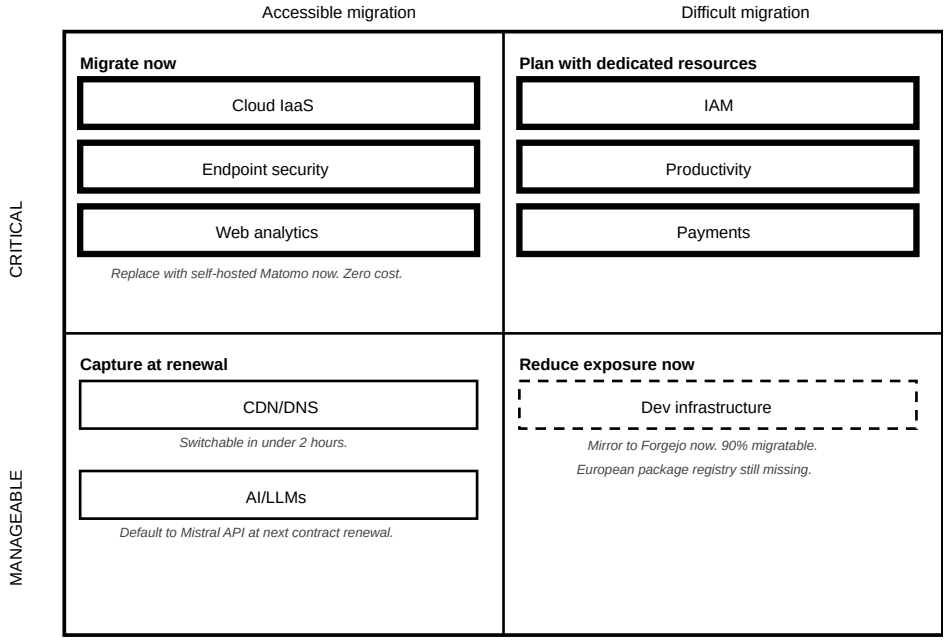
Set the normative floor	Recompose the market	Take structural initiative
EUCS/CADA: sovereignty as eligibility threshold, not a scoring factor	**Joint procurement** framework with pre-qualified sovereign providers	**European public data** as conditional AI training asset: sovereignty of infrastructure as access condition
Interoperable Europe Board: open identity federation, open messaging, ODF for cross-border exchange	**Mandatory exit cost disclosure** at every contract renewal	**Digital Europe Programme:** address the lobbying asymmetry through independent technical expertise funding
DC-EDIC: binding portability floors by layer: cloud, identity, AI	**IPI:** signal reciprocity readiness on U.S. federal tech markets	**Shared sovereign AI compute** via DC-EDIC and EuroHPC mandate extension

None of these instruments requires a political consensus that does not already exist in principle. What is missing is coordinated activation: a critical mass of member states signalling readiness to procure under sovereignty-conditioned frameworks, and Commission willingness to set normative floors rather than voluntary guidelines. The documented migrations and the cost savings they produced establish that the operational risk of action is bounded. The alignment of political momentum, available alternatives, and documented precedent defines the current window.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Executive Summary - Digital Infrastructure Directors and Technical Decision-Makers

European public institutions depend on a small number of American technology platforms for functions central to daily operations. The matrix below maps eight of those dependencies against two questions: how severe is the disruption if access is denied, and how accessible is migration today.



Identity. Deploy Keycloak alongside your current identity provider now. This workstream takes months to stabilise and cannot start late.

Productivity. European stack is production-ready. Blockers are governance, not technology. Three benchmarks by scale: Échirolles (municipal, €350K annual savings on a €1M IT budget); Schleswig-Holstein (30,000 employees, €9M one-time, €15M+ annual savings from 2026); Gendarmerie Nationale (103,000 workstations, 40% TCO reduction).

Cloud. Qualified European providers cover most public sector workloads. The gap is in advanced managed services most organisations do not need.

This week, no approvals: Replace website analytics with self-hosted Matomo (days, €0, closes a documented GDPR violation). Migrate CDN and DNS to a European provider (under 2 hours).

Certification and compliance: bsi.bund.de (C5), cyber.gouv.fr (SecNumCloud), ncsc.nl, cert.pl, ria.ee

Dive deeper: European alternatives by layer (Annex D) and decision ownership with timelines (Annex G).

European Digital Dependencies. Diagnosis and Priorities for Public Sector Decision-Makers
Nicolas Roux, roux.nse@proton.me, First edition, March 2026.
DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

How to read this report

Senior policymakers will find the four decisions that would change the equation at European scale in Section 4, and their institutional owners, current blockers, and progress signals consolidated in Annex G.

Directors of Digital Services and Chief Information Officers will find a prioritisation framework applicable within a standard budget cycle in Section 5, and a full European alternatives table by layer in Annex D.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Table of Contents

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

European Digital Dependencies. Diagnosis and Priorities for Public Sector Decision-Makers
Nicolas Roux, roux.nse@proton.me, First edition, March 2026.
DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

How to read this report

The Introduction, Section 3 (disruption scenarios), and the Conclusion are relevant to both audiences.

Senior policymakers, parliamentarians, and Directors-General will find the structural analysis of why the dependency landscape is difficult to read in Section 1, the four decisions that would change the equation at European scale in Section 4, and their institutional owners, current blockers, and progress signals consolidated in Annex G. European public sector expenditure data is in Annex F. This path covers approximately 40 pages.

Directors of Digital Services and Chief Information Officers will find the layer-by-layer dependency map in Section 2, a prioritisation framework applicable within a standard budget cycle in Section 5, documented migration cases with transferable lessons in Section 6, vendor evaluation criteria in Annex C, and a full European alternatives table by layer in Annex D. This path covers approximately 45 pages.

Annexes C, D, and G are designed to be used as standalone, printable working documents circulated to technical teams independently of the full report.

The full report is the authoritative reference.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

INTRODUCTION

In 2025, the ICC lost access to its operating American tools.

In February 2025, the United States government sanctioned a sitting ICC prosecutor and several senior court officials under Executive Order 14203.[1] The practical consequences were immediate: access to American payment systems, cloud services, email infrastructure, and software licences was cut off. The individuals sanctioned were acting within their formal institutional mandate, under authority conferred by the states party to the Rome Statute, the majority of whom are EU member states. Their institutional functions were disrupted. The technical infrastructure that became unavailable to them is the same infrastructure that European public institutions operate on daily.

Two readings of this event are in circulation and both deserve to be stated plainly. The first holds that the CLOUD Act and related American legal instruments include procedural protections (warrant requirements, conflict-of-law provisions, provider challenge rights) that make coercive use against European institutions unlikely under ordinary circumstances. This is accurate, and this report does not claim otherwise.[2] The second holds that the sanctions targeted named individuals, not an institution, and that describing this as technology being turned against European public bodies overstates the evidence. The factual record is that the individuals sanctioned held institutional roles, were acting on an institutional mandate, and were stripped of access to institutional tools. Whether that constitutes weaponisation of technology or the ordinary operation of a national sanctions regime is a definitional question this report does not aim or need to resolve: the operational implications are the same either way.

The broader context makes the direction of travel legible. On 21 February 2025, the White House issued a memorandum framing EU digital regulation as "overseas extortion and unfair fines and penalties" and directing trade investigations against EU member states that had implemented digital services taxes or regulations affecting American technology companies.[3] On 5 September 2025, following a €2.95 billion antitrust fine against Google, the U.S. administration threatened to open a Section 301 trade investigation to "nullify" what the President described as discriminatory European enforcement actions against American companies.[4] On 23 December 2025, the Secretary of State imposed visa bans on five European individuals, including former EU Commissioner Thierry Breton, citing their roles in the enforcement of the EU's Digital Services Act.[5] Each of these actions is individually contestable as to its intent. Together they describe a consistent position: that American technology companies operating in Europe should not be subject to European regulatory authority, and that the instruments of American foreign policy will be used to make that position felt.

The questions this report is designed to help answer are operational rather than about geopolitical intent: which systems fail first under this kind of pressure, how long recovery takes, and which decisions taken now reduce that exposure. This report maps these dependencies technological layer by technological layer, assesses available European alternatives, and identifies for each the level at which it can most effectively be addressed: organisational, sectoral, or political.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

METHODOLOGICAL NOTE

A note on terminology: what this report means by "dependency"

The term "dependency" is used throughout this report to describe a situation in which a European public (or private) organisation's ability to operate, govern its data, or fulfil its legal obligations is contingent on decisions made by a non-European actor. This encompasses four distinct but related dimensions, each of which is assessed separately in the mapping that follows:

Operational dependency: the organisation cannot perform core functions without continuous access to a specific product or platform. Switching is technically possible but would require a migration of sufficient complexity and duration to constitute a material operational risk.

Jurisdictional dependency: the organisation's data, communications, or infrastructure are subject to the legal reach of a non-European sovereign, regardless of where that data is physically stored or which entity holds the contract. The CLOUD Act is the primary operative instrument of this dimension for the purposes of this report. Section 702 of the Foreign Intelligence Surveillance Act (FISA) compounds the exposure: it authorises surveillance of non-U.S. persons without an individualised court order, a lower procedural threshold than the CLOUD Act applied to a category that includes, by definition, every European public official.

Jurisdictional exposure is not confined to formal legal instruments. Any non-European actor that retains the technical capacity to modify the behaviour of a deployed system, whether through software updates, configuration changes, patch distribution, or licence validation, holds a de facto channel of control over that system's operational continuity. That channel does not require a court order to activate and is not addressed by data residency measures. It is the mechanism through which operational dependency and jurisdictional dependency converge.

Economic dependency: switching costs, contractual lock-in, or the absence of credible alternatives have created a situation in which the organisation has no realistic choice of provider within any procurement horizon it can plan for.

Normative dependency: the organisation has adopted non-European standards, certification frameworks, or compliance baselines in ways that structurally privilege incumbent non-European products in future procurement decisions.

A product or platform is assessed as generating a critical dependency in this report when it creates exposure across two or more of these dimensions simultaneously. Single-dimension dependencies are noted but classified as manageable.

The normative dependency is not mapped layer by layer in Section 2, but it shapes the transition cost of any procurement decision described in this report. Organisations that have structured their security posture, vendor selection criteria, and risk management frameworks around American standards (principally NIST CSF and SOC 2) face a real but finite gap when moving toward European alternatives. That gap is assessable and, where political will exists, bridgeable.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The primary bridge is ENISA's Technical Implementation Guidance, published in June 2025, which provides explicit mappings between NIS2 requirements and ISO/IEC 27001:2022 and NIST CSF 2.0.[6] For organisations already compliant with either framework, the delta to NIS2 is not a restart: it is a documented set of additional obligations, primarily around supply chain risk management, incident notification timelines, and management body accountability.

Each EU member state has designated a national authority responsible for NIS2 supervision and, in most cases, implementation support. In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI) became the competent authority for NIS2 registration and incident reporting when the national transposition law entered into force on 6 December 2025.[7] In France, the ANSSI operates the MonEspaceNIS2 portal[8] for entity registration and MonAideCyber[9] for initial diagnostic assessment. In Spain, the Centro Criptológico Nacional maintains the Esquema Nacional de Seguridad, whose requirements are mapped to NIS2 in ENISA's guidance.[10] The NIS Cooperation Group, which convenes all member state authorities, coordinates cross-border alignment and publishes shared technical guidance.

For procurement officers who have historically used SOC 2 or FedRAMP authorisation as proxies for vendor trustworthiness, the European equivalents are SecNumCloud (France, ANSSI), C5 (Germany, BSI), and ENS (Spain, CCN). These serve the same functional role: a standardised, audited assurance framework for cloud service providers without the jurisdictional dependency that comes with their American counterparts.

What this report covers

The technology layers for which dependency on American actors creates a documented operational risk for European public organisations.

What this report does not cover

Several layers have been deliberately excluded from the scope of this preliminary report:

- **Vertical sector analysis** (healthcare, local government, defence, education): each sector warrants a dedicated mapping given its specific regulatory constraints. This report provides the common analytical framework; sector-specific breakdowns are its natural continuation.
- **Submarine communication cables and physical network infrastructure:** this layer is excluded from the primary scope, but warrants a direct observation. The United States has a consolidated licensing and oversight regime for submarine cables through the FCC, operating under the Cable Landing License Act of 1921 and reinforced by national security review processes formalised under Executive Order 13913. The European Union has no institutional equivalent at Union level: cable oversight is fragmented across national regulators with no coordinated EU licensing or coordination authority, as documented in the European Union Agency for Cybersecurity report[11].

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

- **Hardware and semiconductor supply chains:** covered in depth by existing institutional assessments, to which this report defers. Primary references: Mario Draghi, "The Future of European Competitiveness," European Commission, September 2024, Part B (Semiconductors)[12]; European Chips Act assessments, 2023[13].
- **Defence sector digital infrastructure and military technology ecosystems:** the dependency profile of armed forces and defence ministries is subject to constraints that lie outside the analytical framework of this report. NATO interoperability requirements, operational continuity obligations for weapons systems, and the specific security classification regimes of defence establishments create a dependency structure that is qualitatively different from that of civilian public administration. As recent institutional analysis has noted, European militaries face a distinct set of constraints in this domain, and the question of replacing American software embedded in NATO weapons systems is not one this report addresses or is equipped to address.[14] Defence-sector organisations should treat the analytical framework of section 2 as applicable to their administrative and support functions, not to their operational technology.

A note on scope and the private sector

This report addresses European public organisations as its primary analytical subject. The dependencies it maps are not, however, confined to the public sector. Operators of essential services under NIS2, financial institutions under DORA, critical infrastructure operators in energy, transport, water, and healthcare, whether publicly or privately governed, are subject to the same operational, jurisdictional, economic, and normative exposures documented here. Hospital groups running clinical information systems on Azure face the same CLOUD Act exposure as ministries. Banks whose authentication infrastructure runs on Entra ID face the same IAM dependency as regional administrations.

The analytical framework of section 2, the four dependency dimensions, and the prioritisation logic of section 5 are directly applicable to any European organisation of significant scale. This report does not extend its mapping to private sector operators because each regulated sector warrants its dedicated assessment, given its specific regulatory constraints and dependency profile. It notes the equivalence explicitly so that decision-makers in regulated private entities do not draw a false distinction between the public sector problem documented here and their own exposure.

A note on objectivity

Every private actor, American or European, is assessed against the same criteria. This report has no commercial relationship with any vendor. European alternatives are evaluated with the same rigour applied to the products they are compared against.

Section 1 - A framework for clear thinking

Why the debate on digital sovereignty is difficult to read

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Before mapping the digital dependencies of European public organisations on U.S.-based products, it is necessary to understand why those dependencies are so difficult to assess objectively. Decision-makers are navigating a fog maintained by several overlapping and structurally predictable interests.

1.1 - Vendors have a structural interest in making dependency invisible

Service integration strategies are designed to raise switching costs over time. Platform economics literature extensively documents that switching costs and network effects, while arising organically, are deliberately maintained and extended through interoperability restrictions, proprietary formats, and bundled pricing[15], Microsoft's licensing structure being a canonical example[16]. Proprietary APIs, platform-specific data formats, and bundled licensing structures ensure that the deeper an organisation integrates, the more expensive it becomes to leave, inducing a form of economic dependency, as defined in the methodological note. The EU's own Data Act, adopted in 2023, acknowledges this explicitly[17], describing its objective as making switching between cloud providers "fast, free and technologically fluid", a formulation that implicitly concedes the current situation is none of those things. The practical result is that organisations typically discover the true depth of their dependency only when they attempt to leave.

The marketing language deployed to frame this dependency ("innovation", "efficiency", "best-in-class") presents what is a structural constraint as a rational choice freely made. Meanwhile, the same vendors spend record sums to ensure that the regulatory environment in Brussels remains as favourable as possible to their continued dominance. According to an October 2025 analysis of the EU Transparency Register by Corporate Europe Observatory and LobbyControl (both advocacy-oriented NGOs), the tech industry spent a record €151 million on EU lobbying, with Meta, Microsoft, Apple, Amazon and Google alone accounting for €49 million of that figure.[18] The underlying data are drawn from mandatory public disclosures on the EU Transparency Register. This €151 million figure represents a 33.6% increase in two years. “Big Tech” now employs more full-time lobbyists in Brussels than there are MEPs in the European Parliament[19].

The lobbying effort has extended beyond shaping individual regulations toward reshaping the regulatory environment itself. In November 2025, the European Commission proposed a Digital Omnibus package[20] that would weaken the GDPR's definition of personal data, restrict citizens' right to access their own data held by third parties, authorise training of AI models on sensitive personal data without active consent, and delay implementation of the AI Act by at least twelve months. A comparative analysis by Corporate Europe Observatory and LobbyControl, published in January 2026[21], documents the alignment between these proposed changes and the prior lobbying positions of Google, Microsoft, Meta, and their associated trade organisations. Each change is traceable to a specific public lobbying submission in the EU Transparency Register. The industry has also expanded its parliamentary coalition-building strategy, cultivating relationships with a broader range of political groups than in previous mandates, with the Digital Omnibus as an explicit priority in those engagements[22]. The outcome of the Digital Omnibus legislative process was pending at the time of publication of this report. Its significance for the dependency analysis is

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

structural: the normative dimension of dependency documented in this report (i.e. the adoption of frameworks that privilege incumbent non-European products) is being actively shaped by a well-resourced, strategically coordinated lobbying operation whose methods are now publicly documented.

The institutional response to this pressure is shifting. Henna Virkkunen, Executive Vice-President of the European Commission with responsibility for technological sovereignty, stated publicly in March 2026 that Europe's dependence on American technology had become a security concern visible beyond specialist circles. She explicitly encouraged European individuals and organisations to consider European alternatives, describing them as "not something that we have to lower our expectations for, but something that is high quality, innovative and provides an important level of assurance."[23] A Commission technological sovereignty package is expected in May 2026, drawing on a €234 billion European competitiveness fund, and is described as including a €20 billion AI infrastructure fund, supply chain cybersecurity liability provisions for digital infrastructure, and strong orientation toward sovereign cloud and open-source principles.[24]

1.2 - Consultants and system integrators amplify the dependency

The business model of major European IT consultancies is structurally aligned with American cloud vendors. This alignment operates at two distinct levels, each with its own dynamic.

At the level of large generalist groups, the dependency is a consequence of scale. Capgemini, Atos, Sopra Steria and their peers built European-facing practices around American platforms because those platforms dominated the market their clients operated in. Capgemini holds AWS Emerald-level sponsorship status[25] and in its 2025 full-year results[26], its CEO cited "sovereignty" as a growth driver, noting demand was accelerating "as demonstrated by our recent announcements with AWS, Google and Microsoft." Atos, despite its own positioning as a European digital infrastructure player, describes its managed services offering as built on 'strategic partnerships with AWS, Azure, and Google Cloud.[27] For these firms, recommending American platforms was, and still is, the path of least resistance in a market their clients have already standardised on, and their competency bases, certification pathways, and margin structures have been built accordingly.

At the level of specialist cloud consultancies, the alignment is more explicit and more deeply embedded. Firms whose entire practice is built around a single vendor ecosystem (AWS, Google Cloud, or Microsoft Azure) have no commercial incentive to recommend alternatives. Revenue-sharing arrangements, tiered certification programmes, and margins on licence resale make incumbent recommendation the default output of any engagement. Several of the most active players in this segment, including Devoteam, Claranet, and Xebia, publish their hyperscaler partnerships and revenue targets openly in annual results and press releases. Devoteam, for instance, reported in its 2023 annual results that approximately 50% of its revenue was generated through five strategic partners[28]: AWS, Google Cloud, Microsoft, Salesforce, and ServiceNow, and announced in January 2025 a four-year strategic partnership with Google Cloud targeting $2 billion in revenue for that business unit alone by 2028[29].

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The practical consequence is structural in both cases: an organisation seeking independent advice on European alternatives is unlikely to find it from an advisor whose partnership agreements, certification investments, and margin structures reward the opposite recommendation. The conflict of interest is plainly visible in their annual reports.

1.3 - Chief Information Officers are in a structurally uncomfortable position

The incentive structure facing Chief Information Officers (CIOs) systematically favours inaction over migration. This is a predictable response to a specific set of documented professional constraints[30] [31].

A migration to European alternatives is usually presented as a long, expensive, and operationally complex undertaking. Large IT projects fail or stall at high rates across all categories (industry surveys consistently place the figure at 60 to 70%) and migration projects are not an exception to that norm. The failure of a major IT project is one of the primary documented causes of CIO dismissal. CIO tenure already averages between 3 and 5 years across industries, appreciably below that of CEOs and CFOs. The arithmetic is straightforward: a contested multi-year migration that encounters difficulties puts the CIO's position at direct personal risk, with no guarantee that the organisation will see the benefits before the next leadership cycle begins.

In a stable geopolitical environment, the *status quo* would be a defensible choice. A dependency that has not been activated as a weapon generates no immediate crisis while a failed migration generates one immediately, albeit a controlled one. Absent external pressure, the rational response for an individual CIO is to defer. The ICC case documented in the introduction of this report illustrates the moment at which that calculus inverts. An organisation that has not prepared does not avoid the migration but does lose the ability to conduct it on its own terms, at its own pace, and before the crisis rather than inside it.

The result is a collective action problem. Each individual sourcing decision is locally rational, while the aggregate outcome (a continued and deepening operational and economic dependency, in the terms defined above) is collectively irrational.

This is compounded by a genuine, if partially addressed, lack of visibility. Several European initiatives provide useful reference points: France's SILL (Socle Interministériel de Logiciels Libres), maintained by DINUM since 2013, catalogues 530 open-source tools recommended for public administration[32]. At EU level, the European Commission's Open Source Observatory (OSOR), now integrated into the Interoperable Europe Portal, references over 640 solutions across more than 30 public sector domains[33]. Germany operates a comparable national platform, Open CoDE[34], focused on exchange and reuse of public administration software.

These initiatives are valuable and deserve wider recognition. They are not, however, substitutes for a strategic dependency assessment: they catalogue what exists and what is deployed, they do not systematically evaluate operational maturity against incumbent products, quantify switching costs, or identify residual dependencies within nominally open-source solutions. The conditions for a fully informed migration decision do not yet exist at European scale. This report builds on that existing

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

work to provide what decision-makers more immediately need: a criticality-ranked assessment structured around the question of what to do, in what order, and at what level.

The collective action problem described above is not self-correcting. It persists because the information environment that would be necessary to shift individual decisions does not yet exist. That is a supply-side failure, and it is the subject of the section that follows.

1.4 - European alternatives are poorly documented and insufficiently promoted

The European cloud and software ecosystem is not absent, but it is fragmented. Europe has a rich landscape of cloud providers, managed service operators, telecoms infrastructure specialists, and software publishers, but collectively they lack the scale to compete with global hyperscalers on cost and breadth of capability. This is a coordination problem with deep structural roots: national strategies developed in parallel, procurement frameworks that remained nationally siloed, and regulatory responses that consistently lagged market reality.

The market consequences are measurable. European cloud providers held approximately 22% of the European infrastructure cloud market in 2017. By 2024, that figure had fallen to 15%[35], even as their absolute revenues continued to grow. They are losing ground in their home market while the overall market expands around them.

This fragmentation creates a specific problem for decision-makers: the information environment surrounding European alternatives is unreliable in both directions. Larger European actors, positioned as national champions, tend toward institutional defensiveness, emphasising compliance and data residency while understating genuine capability gaps. Smaller actors, lacking the marketing infrastructure of the incumbents they compete against, compensate with claims that outrun their operational maturity. Neither produces the kind of sober, comparative assessment on which procurement decisions can responsibly be based. This is once again a structural market dynamic: vendors with limited marketing budgets competing against trillion-dollar platforms have few other tools available to them.

There are genuine grounds for optimism, and they deserve acknowledgement. In July 2025, Germany, France, Italy, and the Netherlands established the European Digital Infrastructure Consortium to jointly develop and scale sovereign digital tools[36]. Schleswig-Holstein is migrating 25,000 workstations to OpenDesk, an open-source suite built on Nextcloud and Collabora Online, developed under the auspices of Germany's Centre for Digital Sovereignty. As of late 2025, approximately 80% of the transition is complete, with projected licence cost savings exceeding €15 million in 2026 alone. Following the sanctions documented in the introduction to this report, the International Criminal Court announced in November 2025 that it was replacing its Microsoft office suite with the same platform.

The oldest and most operationally mature example in the French public sector is the Gendarmerie Nationale's GendBuntu project. Beginning in 2005 with a departure from Microsoft Office, and moving to a full Ubuntu-based desktop environment from 2008[37], the Gendarmerie completed its desktop migration in 2014[38]. By 2024, GendBuntu runs on 97% of over 103,000 workstations, with

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

cumulative savings estimated at €50 million by Major Stéphane Dumond (project director), though this figure has not been independently audited. The case is examined in detail in section 6.1.

Both developments signal that the political and institutional conditions for coordinated action are beginning to form. The change management conditions and transferable lessons from both migrations are examined in section 6. These developments do not, however, address the cloud and SaaS dependency layer that now constitutes the primary exposure for most European public organisations.

In November 2025, the American IT services firm Kyndryl announced its intention to acquire Solvinity[39], a Dutch managed cloud provider. Solvinity manages DigiD, the Netherlands' national citizen authentication system, and the Justitienet environment of the Ministry of Justice and Security[40]. The Dutch cabinet raised formal concerns, the Dutch parliament voted to accelerate investment in European cloud alternatives in direct response, and the Netherlands' investment screening authority opened a national security investigation into the acquisition in January 2026[41]. The transaction remains pending as of the date of this report.

The case illustrates a vulnerability that any dependency mapping must account for: a deliberate migration to a European provider does not guarantee lasting sovereignty if that provider is subsequently acquired by a non-European entity. Jurisdictional dependency can emerge after a procurement decision that appeared, at the time, to eliminate it. Ownership provenance is a live variable, not a fixed attribute of a procurement decision.

On 24 March 2026, the Finnish Ministry of Justice announced that Finland's election data would no longer be stored with Amazon Web Services, following a report from SUPO, the Finnish Security and Intelligence Service, that dependence on foreign providers could "undermine sovereignty."[42] The decision is notable both for its source (a national security assessment, not a data protection ruling) and for its timing: a poll published the same day found that 4% of Finns trusted the United States, comparable to the 3% who trusted China. The political conditions for sovereign migration decisions are not uniform across member states, but they are shifting.

1.5 - The problem of "false sovereigns"

The language of digital sovereignty has become a market category. This creates a specific analytical hazard: products and platforms marketed as European, sovereign, or trusted may embed the very dependencies they claim to eliminate. Without a consistent, explicit test applied to each claim, procurement decisions made in the name of sovereignty can deepen operational dependency while providing political cover for inaction.

The pattern is not new. Gaia-X, the flagship European initiative launched in 2020 to build a federated European cloud, is the most documented example of how sovereignty frameworks can be reshaped by the actors they were designed to constrain. American hyperscalers joined the initiative, shaped its governance, and the project's original purpose was progressively diluted. As Cristina Caffarra, Honorary Professor at UCL and former senior official at the European Commission, summarised: "The problem was that American companies lobbied to be included. Once Microsoft,

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Google, and AWS were inside Gaia-X, the initiative lost its purpose."[43] The term 'sovereignty-washing' has since entered the policy vocabulary to describe this dynamic: the use of sovereignty language by actors whose business model depends on the dependencies they claim to resolve. The mechanism is structural rather than necessarily intentional. Gaia-X's governance model allowed American hyperscalers to shape the framework from within, progressively diluting its original purpose.

At the product level, the "cloud de confiance" model developed in France provides the clearest available illustration of both the problem and the attempts to resolve it.

The concept was formalised through France's national cloud doctrine, which conditions access to sensitive public sector data on SecNumCloud 3.2 qualification from ANSSI. SecNumCloud is the most demanding cloud security certification in Europe, covering 276 requirements across 15 chapters including, critically, explicit protection against extraterritorial laws[44]. The framework is technically serious and institutionally rigorous. In normative terms, SecNumCloud represents Europe's most serious attempt to establish an indigenous certification baseline, one that does not defer to American frameworks as its reference point.

Two joint ventures were created to operate within it. S3NS (Thales, majority shareholder, in partnership with Google Cloud) obtained SecNumCloud 3.2 qualification in December 2025[45]. Bleu (Orange and Capgemini, in partnership with Microsoft) has cleared qualification milestones J0 and J1 as of November 2025 and is targeting full qualification in the first half of 2026[46]. Both ventures were created specifically to deploy American cloud technology in structures legally controlled by French entities and operationally isolated from their American partners.

The distance between the original marketing proposition and the current operational reality is instructive. Both ventures were initially described as "sovereign cloud" solutions but are, factually, not sovereign. They are structured legal arrangements designed to mitigate, not eliminate, the jurisdictional exposure created by dependency on American platforms.

The most authoritative institutional statement on the residual jurisdictional risk came not from a cybersecurity agency but from a court. On 20 March 2026, France's highest administrative jurisdiction, the Conseil d'État, rejected challenges to the CNIL's authorisation for the Health Data Hub to host health data of ten million French citizens on Microsoft Azure[47]. In its decision, the court explicitly acknowledged that the risk of access by American authorities "cannot be totally excluded" and validated the authorisation nonetheless, on the grounds that existing safeguards were sufficient for the specific use case and that no credible European alternative was available at the required scale at the time of authorisation. The legal position articulated by the Conseil d'État is precise and has direct implications for procurement decisions across all public organisations: the risk is real, judicially acknowledged, manageable under specific conditions, and neither negligible, nor theoretical, nor resolved by data centre location alone.

ANSSI's Director General, Vincent Strubel, stated explicitly before a Senate inquiry in May 2025 that S3NS and Bleu are "conformant, on paper, with SecNumCloud requirements" and that legal

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

analysis commissioned by ANSSI concludes they are "in principle" immune to the CLOUD Act and FISA[48]. The word "in principle" is load-bearing.

Under the CLOUD Act, Microsoft remains subject to American government data demands regardless of data centre location, with no GDPR exception. GDPR Article 48 requires a formal international agreement as the basis for any foreign court order. No such agreement exists between the United States and the European Union. Unlike the bilateral agreements Washington has concluded with the United Kingdom and Australia, EU organisations currently operate between two irreconcilable and simultaneously binding legal systems. Whether the structural separation of S3NS and Bleu from their American parent platforms is sufficient to defeat CLOUD Act reach has not been tested in court. Thierry Carrez, Executive Director of the OpenInfra Foundation, assessed the situation precisely: "U.S. hyperscalers are trying to find a mix of technical solutions and legal engineering to isolate their EU products from potential demands from the U.S. government. This is a positive development, but whether that mix will prove sufficient is unsure and untested."[49]

This report treats this open legal question as exactly what it is: open. S3NS and Bleu represent a serious structural effort to address the problem of American jurisdictional reach. They are not false sovereigns in the dismissive sense, they have invested substantially in separation architectures that earlier products did not attempt. But they are not substitutes for European-owned, European-operated, and European-developed platforms when the use case demands full jurisdictional certainty.
The test applied in this report is therefore binary: does the product's sovereignty claim rest on a structural legal argument that remains untested under adversarial conditions, or does it rest on the absence of American corporate ownership in the chain? These are different things, and treating them as equivalent is the analytical error this section is designed to prevent.

1.6 - The false equivalence argument

A recurring objection to the migration agenda documented in this report takes the following form: replacing American platforms with European alternatives does not resolve dependency, it merely substitutes one dependency for another. If European cloud providers are themselves dependent on American semiconductor supply, if open-source foundations are governed by U.S.-based non-profits, and if the global software package registry infrastructure is American-controlled, then the sovereignty gain from migration is illusory.

The objection deserves a direct response, because it is sometimes legitimate and sometimes, whether deliberately or not, functioning as a justification for inaction.

Where it is legitimate: the report acknowledges these residual dependencies explicitly and without qualification. Sections 2.7 and 3.3 document the semiconductor dependency on NVIDIA and AMD GPU architectures. Section 2.8 documents the package registry dependency on npm, PyPI, and Docker Hub. Section 2.1 documents the Ontario court ruling against OVHcloud. None of these dependencies are concealed, and the report does not claim that European alternatives eliminate all exposure. What it claims is that they eliminate the most acute exposures (jurisdictional reach under

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

the CLOUD Act, contractual lock-in to proprietary platforms, and the kill-switch IAM dependency) while the residual dependencies are of a different kind, structurally less acute, and addressable through the instruments described in section 4.

Where it produces inaction: the argument is sometimes framed as a binary: either full sovereignty or none. That framing renders any partial improvement worthless and justifies continued dependency on the current incumbents. Whether this is the intended purpose or an unexamined consequence is, for the organisations whose dependencies deepen with each passing procurement cycle, a distinction without operational significance. The result is the same: inaction that is measurably costly, that strengthens existing lock-in, and that narrows the options available to European institutions at the next point of decision. The appropriate analytical response is not to dismiss the residual dependencies the argument identifies, which this report documents explicitly, but to reject the binary framing that treats their existence as grounds for doing nothing. Reducing four dimensions of simultaneous dependency to one or two residual dependencies is a material improvement, even if it is not a complete solution. An organisation that has migrated its IAM to Keycloak on UpCloud, its productivity suite to Nextcloud on Hetzner, and its endpoint security to WithSecure is not fully sovereign in any absolute sense. It is, however, in a structurally different position from one that runs Entra ID, Microsoft 365, and CrowdStrike simultaneously: the number of decision points outside European legal control has been reduced from a dozen to two or three, and the remaining ones are of a qualitatively different nature.

The specific question of Chinese technology dependency is worth addressing directly. The European public sector has no comparable operational dependency on Chinese technology platforms in any of the eight layers mapped in section 2. Chinese providers do not operate in the IAM, productivity, cloud IaaS, endpoint security, or CDN markets for European public administrations in any documented way. The semiconductor dependency on NVIDIA and AMD documented in section 2.7 is real, but it is a supply chain dependency shared with the Chinese AI ecosystem itself, which is navigating the same structural constraint from the opposite direction. The policy implication is not that European AI infrastructure should seek Chinese semiconductor alternatives but that the EU Chips Act targets a genuine and shared structural dependency whose resolution requires a decade-long industrial commitment rather than a procurement decision.

Two further objections circulate in the policy debate and deserve acknowledgement. The first, articulated publicly by the chief executive of Siemens in March 2026, holds that requiring companies to develop AI on European systems would slow innovation by separating European development from the global frontier.[50] This objection is worth taking seriously in its strongest form: European AI infrastructure is not yet at parity with the largest American commercial facilities, and organisations with genuine frontier AI requirements face a real capability trade-off. The report does not argue otherwise. What it argues is that the majority of European public sector AI workloads are not frontier AI applications. Document analysis, citizen correspondence processing, administrative classification, and decision support for benefit processing do not require the most powerful models in the world. They require models that are adequate, auditable, and sovereign.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Mistral's open-weight models meet that specification today. The frontier capability gap is a real constraint for a minority of use cases and an irrelevance for the majority.

The second objection concerns defence: European militaries use American software embedded in NATO weapons systems, and replacing it is not operationally feasible. This is accurate and this report does not contest it. As noted in the methodological section, defence sector digital infrastructure is outside the analytical scope of this report precisely because its constraints are qualitatively different from those of civilian public administration. The objection is legitimate in its domain. It becomes a false equivalence when it is used to argue that civilian administrations should not migrate their email and file storage because fighter jets cannot change their avionics software.

The analytical test applied throughout this report is consistent: does a migration reduce documented exposure across the four dependency dimensions defined in the methodological note, while avoiding the creation of a new dependency of comparable or greater severity? For the European alternatives assessed in section 2, the answer is yes across all eight technological layers, subject to the residual dependencies explicitly documented in each case. That test, applied rigorously and without commercial preference, is the appropriate response to the false equivalence argument.

Section 2 - A layer-by-layer dependency map

A note before mapping: the wrong question and the right one

The instinctive framing for a dependency mapping of this kind is: which European provider can replace AWS? That is the wrong question, and this report does not attempt to answer it.

No European provider will replicate the full AWS service catalogue. That catalogue was built over twenty years by a company with access to essentially unlimited capital, operating in a continental domestic market with no regulatory friction. The conditions that produced it do not exist in Europe and will not be manufactured by policy. Asking for a European AWS is asking for a different history.

The right question is different: for each layer, what does a given organisation actually need, and is a credible European alternative available for that specific need? The answer to that question varies significantly by organisation type. A national statistics agency running large-scale data pipelines has fundamentally different requirements from a regional prefecture managing administrative workflows. A university hospital operating clinical imaging systems is not in the same migration conversation as a mid-sized municipality digitising planning applications.

This report therefore assesses each layer against a spectrum of organisational profiles, not against a single hypothetical maximum-demand user. For each layer, the assessment distinguishes between:

- **Core workloads**: compute, storage, identity, collaboration, and communication functions that virtually every public organisation depends on and for which European alternatives exist at production maturity today.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

- **Advanced workloads**: managed AI/ML pipelines, large-scale analytics, serverless architectures at high concurrency, and specialist developer tooling for which European alternatives are emerging but not yet uniformly mature.

The migration conversation for the vast majority of European public organisations is concentrated in the first category. The gap in the second category is real but not the blocker it is routinely presented as. Presenting it as such serves the incumbents more than it serves the organisations considering migration.

Analytical framework

Each technological layer is assessed against a consistent set of seven dimensions. These are structural assessment rubrics, distinct from the four dependency dimensions (operational, jurisdictional, economic, normative) defined in the methodological note. Those four dimensions classify the nature and severity of each exposure. These seven organise how each technological layer is examined.

- **Critical function:** what the layer actually enables in operational terms.
- **Dominant U.S. actor(s):** and the structural reasons for their dominance.
- **Dependency level:** rated CRITICAL, SERIOUS, or MANAGEABLE according to the criteria below.
- **Existing EU alternatives:** assessed honestly on current maturity, market share, and capacity to absorb migration at scale. The order in which they are presented in each sub-section is arbitrary and does not necessarily represent the maturity of the product or company.
- **Residual dependencies**: American components embedded within nominally EU solutions.
- **What holds:** the resilience that exists today without additional preparation, under the pressure scenarios examined in section 3.
- **What is missing:** the technical, economic, or political blockers to credible EU alternatives at scale.

The **Dependency level criteria** ratings correspond to the following definitions:

- CRITICAL: failure or denial of service would halt core public service delivery within hours or days, with no available fallback.
- SERIOUS: significant operational degradation would result; workarounds exist but are costly, slow, and unsuitable as permanent solutions.
- MANAGEABLE: impact is real but contained; migration is feasible within normal budget and planning cycles without requiring exceptional political commitment.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

2.1 - Cloud infrastructure and compute

Critical function: provision of the computing capacity, storage, and managed platform services on which virtually all other digital operations depend. This layer is the substrate. Email, collaboration tools, databases, application hosting, and backup systems all run on top of it. Loss or denial of access at this layer is not a degradation but a total cessation of service.

Dominant U.S. actors: Amazon Web Services, Microsoft Azure, Google Cloud Platform.

Dependency level: CRITICAL

AWS, Azure, and GCP collectively hold approximately 70% of the European cloud market[51], with U.S. providers as a whole accounting for roughly 85% when smaller American vendors are included. Their dominance is the product of a decade of aggressive pricing, global network effects, and first-mover advantage in the managed services layer. The lock-in is architectural: organisations have built dependencies on platform-specific services (Lambda functions, BigQuery pipelines, Azure Cognitive integrations) that have no direct drop-in replacement. Infrastructure can be migrated but application architecture cannot be switched without rethinking.

Existing EU alternatives

At the core IaaS layer (compute, storage, networking, and container orchestration) a mature European market exists. The primary players are:

OVHcloud (France): the largest European cloud provider by revenue, operating 43 data centres globally. Competitive bare-metal and object storage offering, SecNumCloud-qualified infrastructure available. Revenue approximately €900 million in 2024.

Scaleway (France): developer-focused, strong GPU and Kubernetes offering. Primary infrastructure partner for Mistral AI[52].

Hetzner (Germany): exceptional price-to-performance ratio. Dominant in cost-sensitive developer and public sector workloads. No managed services beyond core compute and storage, which is a constraint for complex architectures and an irrelevance for simple ones.

IONOS (Germany): enterprise-oriented, strong SME and public sector presence across Europe. Full EU data residency.

Open Telekom Cloud / T-Systems (Germany): targeting regulated industries and government. Offers a broad managed services catalogue by European standards, with sovereign cloud options for federal and Länder public sector.

STACKIT (Germany, Schwarz Group): designed for enterprise workloads with full EU data isolation. Growing adoption in retail and logistics sectors.

Beyond the Franco-German core, the European IaaS landscape includes **UpCloud** (Finland, 13 data centres across four continents, ISO 27001 certified, CISPE member), **Exoscale** (Austria, operated by A1 Telekom Austria, seven data centres across five European countries), **Aruba Cloud** (Italy, founding CISPE member, data centres across Italy, Czech Republic, France, Germany, Poland, and

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

the UK), and **Leaseweb** (Netherlands). These providers serve primarily national and regional markets, but collectively extend the geographic diversity of the European IaaS alternative base beyond the Franco-German axis.

For core workloads (hosting, storage, virtual machines, managed Kubernetes, basic database services) these providers collectively cover the requirements of the overwhelming majority of European public organisations today.

Residual dependencies

The legal literature on the CLOUD Act offers a more measured picture than either its proponents or its critics typically present. The Act requires a court order or warrant before any disclosure can be compelled. It includes conflict-of-law provisions that theoretically allow providers to challenge requests when compliance would violate the law of another country, and it establishes a framework for bilateral executive agreements that would subject American requests to oversight by foreign governments.[53] The Congressional Research Service notes that the Act "attempts to address conflicts between U.S. law and foreign data protection laws" through these mechanisms.[54]

Two structural limitations, however, constrain what these protections can actually deliver. First, in the absence of an executive agreement between the United States and the European Union, the bilateral review mechanism does not apply. No such agreement has been concluded as of the date of this report.[55] Second, the Act's conflict-of-law provisions presuppose that the provider will challenge the request. A provider's willingness and capacity to mount that challenge depends on commercial and legal calculations that lie entirely outside the control of the European institution (or company) whose data is at issue. The procedural architecture of the CLOUD Act functions as intended when the political relationship between the United States and a given country is stable and cooperative. The question this report raises is what happens when that assumption no longer holds. A question the legal literature, written largely before 2025, does not fully address.

Extraterritorial jurisdictional reach is not an exclusively American instrument either. In April 2024, the Royal Canadian Mounted Police issued a Production Order targeting subscriber data stored by OVHcloud on servers in France, the United Kingdom, and Australia, bypassing the Mutual Legal Assistance Treaty process between Canada and France.[56] OVHcloud, a French company operating under French law, invoked France's blocking statute. On 25 September 2025, Justice Heather Perkins-McVey of the Ontario Court of Justice rejected that challenge, ordering disclosure and determining that national security considerations took precedence.[57] French law prohibits this type of data transfer outside formal treaty channels, with penalties up to €90,000 and six months' imprisonment for non-compliance. The case places OVHcloud in a structurally irresolvable conflict between two legal systems, and OVH filed an appeal (pending at the time of writing of this report). Any provider with subsidiaries or legal presence in a foreign jurisdiction is exposed to analogous pressure through that jurisdiction's own legal instruments. Sovereignty of storage location is a necessary but not sufficient condition for data protection. Sovereignty of corporate structure matters equally, must be evaluated at procurement time, and monitored thereafter.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

What holds

European public organisations running core workloads on bare-metal infrastructure at a European provider with no American shareholders (OVHcloud, Hetzner, STACKIT) are operationally resilient to political pressure and targeted commercial suspension. The Ontario ruling does not affect OVHcloud's EU operations under French law. The resilience that OVH rightly claims applies specifically to workloads hosted in EU data centres under French-law contracts. No decision taken in Washington can interrupt a virtual machine running in a French or German data centre under a contract with a European entity. The resilience does not extend to architectures that depend on platform-specific managed services: a workload built on AWS Lambda or Azure Cognitive Services has no equivalent to switch to under pressure. The distinction between infrastructure dependency and architectural dependency is the first variable any organisation must resolve before claiming resilience at this layer.

What is missing

The gap between European and American providers is real but concentrated. It sits primarily in three areas:

At the **advanced workload layer:** managed AI/ML pipelines, serverless functions at high concurrency, and the breadth of database engine support available on AWS or Azure have no European equivalent of comparable catalogue depth. For organisations with workloads in this category, migration requires architectural rethinking, not just provider substitution. This is a genuine constraint for a minority of public sector organisations and an irrelevance for the majority.

At the **investment scale:** OVHcloud's total 2024 revenue is approximately 0.9% of AWS's annual revenue. The R&D and infrastructure investment capacity implied by that ratio cannot be closed through organic growth alone. Coordinated public investment at EU or member state level is a prerequisite for closing it.

At the **managed services coordination layer**: European providers operate excellent but largely siloed platforms. A multi-provider European architecture, combining OVHcloud compute with Scaleway GPU capacity and Hetzner storage, for instance, is technically feasible but requires integration work that a single hyperscaler relationship does not. This is solvable through open standards and interoperability frameworks, but it requires deliberate architectural choices that organisations accustomed to single-vendor convenience are not always prepared to make.

Investment signal

European sovereign cloud IaaS spending is projected to more than triple from $6.9 billion in 2025 to $23.1 billion in 2027, at which point Europe is forecast to surpass North America in sovereign cloud spending. Gartner estimates that geopatriation projects will shift 20% of current workloads from global to local providers by 2027[58]. Demand is forming faster than supply. The policy and investment decisions taken in the next few years will determine whether European providers are positioned to absorb that demand, or whether it flows back to American hyperscalers operating European-branded sovereign wrappers.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

2.2 - Identity, Authentication and Access Management (IAM)

Critical function: determination of who can access what, across every system an organisation operates. IAM is the control plane of the entire digital infrastructure. Every other layer depends on it: cloud access, email, collaboration tools, internal applications, VPNs, and developer pipelines all authenticate through an identity provider. A failure or denial of service at the IAM layer does not degrade specific services, it locks users out of everything simultaneously.

Dominant U.S. actors: Microsoft Entra ID (formerly Azure Active Directory), Okta, Auth0 (acquired by Okta in 2021).

Dependency level: CRITICAL

The global identity and access management market was valued at $25.96 billion in 2025 and is forecast to reach $42.61 billion by 2030, with North America accounting for the largest regional share.[59] The vendors that dominate enterprise deployments are, with marginal exception, American: MarketsandMarkets identifies Microsoft, Ping Identity, and IBM as the market's leading operators, with Okta, Oracle Identity Governance, and CyberArk accounting for the majority of remaining enterprise contracts.[60] No European vendor appears in any tier of the competitive landscape. For European public administrations, this means that the layer of infrastructure responsible for authenticating every user and authorising every access decision is, in most cases, operated by a vendor incorporated in the United States and subject to American law.

Any organisation on Microsoft 365 is, by construction, already running Entra ID as its identity provider. The European Commission has been investigating[61] whether this bundling constitutes an abuse of dominant position, following complaints that Microsoft's licensing practices cost European businesses and public sector organisations up to €1 billion annually. In November 2024, the U.S. FTC opened a parallel investigation into the same practices.[62]

The strategic sensitivity of this layer is compounded by a property it shares with no other: IAM dependency is invisible in normal operations and total in failure. An organisation discovers its IAM dependency not when costs increase or performance degrades, but when access is denied. It represents an actionable « kill switch ».

Existing EU alternatives

The primary European-origin alternative is **Keycloak**, an open-source IAM platform originally developed under Red Hat's stewardship and now a Cloud Native Computing Foundation project. Keycloak is functionally mature, supporting the full range of enterprise authentication requirements: multi-factor authentication, single sign-on, the open identity protocols on which inter-organisational access control depends, and financial-grade security standards used in regulated sectors. Version 26.4, released in late 2025, adds passkey support. It is production-deployed at scale in government agencies, banks, and large enterprises globally.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

A technical boundary requires explicit statement. Entra ID and on-premises Active Directory serve overlapping but distinct functions. Active Directory manages domain-joined machine authentication via Kerberos, group policy enforcement, directory services for network resources, and trust relationships between organisational domains. Those are functions for which FreeIPA (open source, stewardship transferred from Red Hat to the community) and Samba AD are the established production-viable alternatives. Keycloak addresses a different layer: web application single sign-on, OAuth2 and OpenID Connect federation for cloud services, and inter-organisational identity brokering. The dependency documented in this section is specifically on Entra ID as a cloud identity provider: the layer through which Microsoft 365 access, SaaS authentication, and B2B federation are managed. Keycloak is the relevant alternative for that layer. Organisations operating on-premises domain infrastructure should assess FreeIPA or Samba AD separately, as neither Keycloak nor any managed cloud identity service replaces domain controller functions. Smaller organisations (typically those below 5,000 agents) frequently operate on Active Directory without Entra ID, which produces a different dependency profile: lower jurisdictional exposure on the identity layer, but a migration path that must address domain infrastructure first before cloud identity can be substituted.

The constraint is not functional maturity but operational overhead[63]. Self-hosting Keycloak at production scale requires dedicated IAM engineering capacity: configuration, high-availability clustering, database management, certificate rotation, security patching, and monitoring. For organisations without that capacity, a managed Keycloak service resolves most of this overhead. European managed Keycloak providers include **Inteca** (German), **Cloud-IAM** (French), and **Clever Cloud** (French). **RCDevs** (Luxembourg) offers WebADM, a European-developed multi-factor authentication and identity management platform that can operate entirely on-premises and federate with both Entra ID and Keycloak. It is positioned specifically for organisations requiring offline functional continuity of authentication under NIS2 resilience obligations. These are not hyperscaler-grade SaaS operations, but they are production-viable for the workload profiles of most European public organisations. The ownership status of each is European as of the date of this report. As the Solvinity case documented in section 1.4 establishes, that status requires active monitoring at each procurement renewal: a provider that passes the ownership test today may not pass it at the next review cycle.

For simpler use cases, particularly citizen-facing authentication for public services, LemonLDAP::NG, developed by the French public sector consortium OW2, is a mature, widely deployed alternative with an established track record in French public administration.

The B2B federation problem

This is both the most significant and least discussed dimension of IAM dependency.

An organisation that has fully migrated its internal identity infrastructure to Keycloak retains a residual dependency on Microsoft Entra ID the moment it needs to authenticate users from partner organisations. Inter-organisational authentication (contractors accessing procurement systems, inter-ministerial collaboration, joint project environments, public-private partnerships) relies on identity

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

federation, the technical mechanism that allows one organisation's authenticated users to access systems operated by another without creating duplicate accounts, built on open protocols that both identity providers must support.

Because Microsoft Entra ID is the dominant enterprise identity provider across European public and private organisations, the majority of B2B authentication chains pass through it by default. An organisation running Keycloak that needs to grant access to users from a partner running Entra ID must either maintain a federation trust with Entra ID or require the partner to create local accounts, the latter being operationally impractical at scale. The result is that full IAM sovereignty at the individual organisation level does not translate into IAM sovereignty at the inter-organisational level, as long as Entra ID dominates the wider ecosystem.

No single organisation can solve this through its own procurement decisions. It is a collective problem requiring coordinated adoption of open identity federation standards across European public administrations. The eIDAS 2.0 regulation and the European Digital Identity Wallet framework are moving in this direction[64], but the gap between regulatory intent and operational deployment remains wide.

Residual dependencies

Keycloak itself has no American corporate ownership: it is governed by the CNCF, a Linux Foundation project. The Red Hat build of Keycloak, which provides enterprise support and hardened releases, is a Red Hat product, and Red Hat is owned by IBM. Organisations requiring full independence from American corporate ownership should use the community build with European managed hosting, accepting the support model trade-off that entails.

What holds

An organisation that has migrated its internal identity infrastructure to self-hosted Keycloak on European cloud retains full internal access continuity under commercial pressure scenarios: no American vendor decision can revoke its users' access to internal systems. What does not hold is inter-organisational authentication. As long as partner organisations (ministries, contractors, other public bodies) operate Entra ID as their identity provider, external authentication chains pass through Microsoft infrastructure by default. Under pressure, the first thing that breaks is the ability to collaborate securely with anyone outside the organisation's own perimeter.

What is missing

Two gaps stand between the current European IAM landscape and full operational sovereignty.

The first is a managed Keycloak offering at the scale of the largest public administrations. European managed Keycloak providers exist and are production-viable for the workload profiles of most European public organisations (Inteca, Cloud-IAM, Clever Cloud). The gap is specifically at the upper end: a fully managed service with the SLA guarantees, support model, and procurement vehicle that a ministry or large regional administration requires. That gap is a market opportunity, not a technical limitation.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The second, and structurally more complex, is the inter-organisational federation problem. Resolving it requires not a product but a standard: a shared European public sector identity federation framework, mandatory for public administrations, built on open protocols, and interoperable by design. The eIDAS 2.0 Digital Identity Wallet provides part of the answer for citizen-facing authentication, however the equivalent for machine-to-machine and B2B administrative authentication does not yet exist at European scale.

2.3 - Endpoint security and threat detection

Critical function: detection and neutralisation of threats on workstations, servers, and devices at the operating system level. Endpoint Detection and Response platforms are deployed at the kernel level of every protected system, with access to processes, memory, file operations, and network activity in real time. They are among the most deeply integrated components in any organisation's IT stack.

Dominant U.S. actors: CrowdStrike (Falcon), Microsoft (Defender for Endpoint), SentinelOne, Palo Alto Networks (Cortex XDR), Splunk (now Cisco).

Dependency level: CRITICAL

Microsoft holds approximately 40% of the endpoint protection platform market according to Gartner's 2024 Magic Quadrant[65], with CrowdStrike second at approximately 14%. Combined, American vendors control the overwhelming majority of enterprise endpoint security deployments in Europe. The dominance is structural: Microsoft Defender for Endpoint is bundled into Microsoft 365 enterprise licences, making it the default choice for any organisation already standardised on the Microsoft stack. CrowdStrike and SentinelOne have been pre-installed by default on hardware from Dell and Lenovo respectively in enterprise configurations[66], further embedding American vendors into procurement chains that European organisations never explicitly chose.

The dependency is compounded by a structural paradox that merits explicit statement: European public organisations are routinely outsourcing the security of their most sensitive systems to actors whose telemetry infrastructure, update mechanisms, and corporate structure are subject to U.S. jurisdiction. An Endpoint Detection and Response (EDR) platform has kernel-level access to every protected endpoint. The data it collects (process trees, file operations, network connections, user activity) is among the most sensitive operational intelligence an organisation generates. Routing that telemetry through cloud infrastructure subject to the CLOUD Act is a documented jurisdictional exposure at the deepest layer of the IT stack.

The kernel-level access problem

The July 2024 CrowdStrike outage[67] demonstrated what kernel-level access means in practice. CrowdStrike's Falcon sensor operates as a Windows kernel boot driver, a component so deeply integrated that Windows cannot start without it[68]. Estimated financial losses to U.S. Fortune 500 companies alone reached $5.4 billion. No European organisation has yet faced a targeted suspension

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

of comparable scope. The absence of a recorded cost reflects the absence of a direct activation event, not a lower exposure to one. No cyberattack had occurred. A single configuration file update from a Texas-based vendor, pushed automatically to millions of systems, had halted public services, hospitals, airports, and emergency services across Europe with no European authority holding any contractual or operational lever to accelerate recovery.

The incident is not a reason to avoid kernel-level security tools: effective threat detection requires deep OS access. It is a reason to ensure that the vendor providing that access is subject to governance frameworks compatible with European operational sovereignty.

Existing EU alternatives

The European endpoint security landscape is more advanced than is generally recognised, and significantly more advanced than it was three years ago.

Bitdefender (Romania) serves public sector clients across Europe with its GravityZone platform, which includes EDR, XDR, and managed detection capabilities, and explicitly targets NIS2 and GDPR compliance requirements.

ESET (Slovakia, founded 1992) is one of the oldest European cybersecurity companies, with a particularly strong presence in Central and Eastern European public administrations. ESET Inspect, its EDR/XDR product, supports on-premises deployment, a relevant differentiator for organisations applying the jurisdictional test strictly.

HarfangLab (France, founded 2018) is the most credible European EDR for regulated and public sector use. It is the first and currently only EDR to receive both ANSSI CSPN qualification (first obtained 2020, renewed and extended to cover both agent and manager in 2024, upgraded to full ANSSI qualification in December of the same year) and BSI certification from Germany's Federal Office for Information Security (BSZ certification, 2025)[69]. In MITRE ATT&CK Evaluations 2024, HarfangLab detected 100% of attack techniques across all 16 attack steps. It supports cloud, hybrid, on-premises, and SecNumCloud deployment modes, offers full data sovereignty options, and is deployed across hundreds of public and private sector clients including sensitive French public administrations. The ANSSI qualification is explicitly recognised by the BSI[70] under mutual recognition agreements, making it the first EDR with dual French-German government certification.

Sekoia.io (France) is primarily a threat intelligence and XDR platform rather than a pure EDR, but its SOC platform integrates natively with HarfangLab, Stormshield, Tehtris, and other European EDR agents, providing a European detection and response layer that can operate above American or European endpoint agents. Named a Leader in the Frost & Sullivan Radar for XDR in 2023[71], referenced in Gartner emerging technology reports in 2024. ANSSI-approved.

Stormshield (France, subsidiary of Thales) provides endpoint protection focused on highly regulated environments including defence and critical infrastructure. ANSSI-qualified. Covers Windows, Linux, and industrial control system environments. Strong in air-gapped and classified environments.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Tehtris (France) offers a full XDR platform covering endpoint, network, email, and cloud, with deployments across European government and critical infrastructure clients. ANSSI-referenced. Strong automated neutralisation capabilities without requiring human intervention.

WithSecure (Finland) offers Elements EDR with full GDPR compliance, European data residency, and documented detection performance. AV-TEST certified for Advanced EDR in 2024[72], successfully detecting all techniques across both APT18 and multi-group attack scenarios. Deployed in European public and private sector. Part of F-Secure's enterprise division, spun out as an independent entity in 2022. WithSecure positions its offering explicitly around NIS2 compliance and European data residency.

Residual dependencies

Two residual risks apply across all European alternatives. First, threat intelligence feeds: all EDR platforms, European and American, draw on global threat intelligence databases. Several European providers source indicators of compromise partially from American threat intelligence services. The degree of dependency varies by provider and is not always disclosed. Second, operating system integration: European EDRs running on Windows still depend on Microsoft's kernel architecture and driver signing processes. This is not a European-specific constraint, as it applies universally, but it does mean that OS-layer sovereignty is bounded by Microsoft's decisions about kernel access, a dynamic Apple demonstrated by closing off macOS kernel access in 2020[73] and moving security vendors to its Endpoint Security Framework.

What holds

An organisation running WithSecure, ESET, Bitdefender, HarfangLab or Tehtris on European-hosted infrastructure retains full security coverage under scenarios in which American vendor licences are suspended or telemetry routing to U.S. infrastructure is interrupted. Detection capability does not depend on American platform availability. The irreducible constraint is OS-layer architecture: European EDRs running on Windows depend on Microsoft's kernel model and driver signing processes, a dependency shared universally and not resolvable at the procurement level.

What is missing

The gap between European and American endpoint security actors is narrowing but remains real in two areas. The first is telemetry scale: CrowdStrike and SentinelOne process threat telemetry from hundreds of millions of endpoints globally, feeding machine-learning models that benefit from scale effects in threat detection. European providers operate at a fraction of that telemetry volume. This is a genuine capability difference for zero-day detection at global scale, and a manageable limitation for most European public sector threat profiles, which are targeted by nation-state actors and ransomware groups whose techniques are usually well-documented rather than genuinely novel. The second is managed detection and response capacity: the European market for qualified MDR providers operating on European EDR stacks is growing but remains thin outside France and Finland. Organisations without internal Security Operations Center (SOC) capacity may find managed service options limited.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

2.4 - Productivity and collaboration

Critical function: document creation and editing, email, calendar, video conferencing, instant messaging, and file storage, i.e. the core operational layer of daily public sector work. Unlike infrastructure layers whose failure is visible only in a crisis, productivity tools are in active use every working hour by every agent. Dependency at this layer is simultaneously the most visible to end users and the most politically sensitive to migrate.

Dominant U.S. actors: Microsoft 365 (Word, Excel, PowerPoint, Outlook, Teams, SharePoint, OneDrive), Google Workspace.

Dependency level: CRITICAL

The existence of European alternatives at production maturity reduces long-term mitigation risk, but does not reduce the current dependency level. Migration, while operationally complex, does not require rebuilding application architectures or replacing infrastructure. It requires organisational change, change management, and procurement discipline. That distinction matters for prioritisation, but not for an assessment of the current situation.

The scale of the dependency is exceptional. According to the Open Cloud Coalition's analysis of European public procurement data from Tenders Electronic Daily, Microsoft holds approximately 77% of the EU public sector productivity software market[74], reaching 90% or above in office productivity software in specific member states. Incidence shares (measuring how frequently Microsoft is named in public procurement notices) rose from a range of 72% to 91% in 2023 to 89% to 100% in 2024. The German federal government alone spends €481 million annually on Microsoft licences at the federal level, with total spending across German states speculated by a member of the Bundestag as "certainly even higher"[75]. European organisations collectively spend an estimated €265 billion (estimation by the Asterès cabinet[76]) annually on U.S. software and services. Microsoft Teams has become the default internal communication tool in government agencies, hospitals, and public administrations across the EU.

Existing EU alternatives

The European productivity landscape is anchored by three complementary platforms for the general use case, as well as alternatives for more specific use cases.

Nextcloud Hub (Germany, founded 2016) is the most widely deployed open-source content collaboration platform in the world according to a 2021 European Commission report, with an estimated 400,000 server instances globally[77]. Nextcloud Hub integrates file storage, collaborative document editing, video conferencing (Talk), messaging, calendar, and email in a single platform. It is self-hostable, cloud-deployable, and available as a managed service through European hosting partners including IONOS, OVHcloud, and Deutsche Telekom. Hundreds of municipal, state, federal, and EU government organisations currently use it. The Austrian Federal Ministry for Economic Affairs deployed it in October 2025[78]. The European Data Protection Supervisor runs on

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

it. In November 2025, Nextcloud announced a €250 million investment in digital sovereignty through 2030. Nextcloud Hub integrates with Collabora Online for document editing.

Collabora Online (UK/Germany, based on LibreOffice) provides browser-based collaborative editing of office documents with strong compatibility with Microsoft Office formats. It is the document engine integrated by default in Nextcloud Hub and is deployed across numerous European public sector organisations. It is the basis of the OpenDesk suite adopted by Schleswig-Holstein and, following the ICC sanctions, by the International Criminal Court.

For video conferencing specifically, **Jitsi** (open source, originally developed by a Romanian engineer, now maintained by 8x8 with European self-hosted deployments widely available) and **BigBlueButton** (open source, widely deployed in European education) provide credible alternatives for organisations not requiring full suite integration.

CryptPad (France, developed by XWiki SAS with EU research grant funding) provides end-to-end encrypted collaborative document editing, an option relevant for organisations handling classified or legally privileged material where the encryption architecture itself is a sovereignty requirement.

The email infrastructure dependency is worth considering by itself. Microsoft Exchange Online is the most widely deployed email platform in European public administration and is, in many organisations, the first Microsoft service to be identified for migration and the one that generates the most specific technical and organisational challenges. The dependency is distinct from the document editing or video conferencing layers because it encompasses not only live communications but historical archives, calendar data, and directory-integrated workflows whose migration requires careful sequencing.

The European alternatives landscape for institutional email is mature. **Open-Xchange** (Germany, founded 2005) is the most widely deployed European groupware backend in the telecommunications and public sector markets. It was the platform to which Schleswig-Holstein migrated its 40,000 mailboxes and calendar entries in the six-month operation completed in October 2025. **Postfix** combined with **Dovecot** constitutes the open-source mail transfer and retrieval stack underlying most self-hosted European mail environments, including OVHcloud's managed email infrastructure. **Kolab** (Switzerland) provides a privacy-focused enterprise groupware platform with strong GDPR-by-design credentials and active public sector deployments in German-speaking administrations. **Blue Mind** (France) offers an enterprise groupware suite with commercial support and native CalDAV/CardDAV (calendar) interoperability.

The specific risks at the email layer extend beyond operational continuity. Email archives hosted in Exchange Online are stored in Microsoft's proprietary PST format and in Outlook-specific folder structures that create extraction friction on exit. Calendar and contact data are subject to the same CLOUD Act exposure as any other Microsoft-hosted data category. For administrations whose email correspondences include inter-ministerial communications, legal proceedings, or citizen data, this combination of format lock-in and jurisdictional exposure makes the email layer a priority for the Quadrant 1 or 2 assessment defined in section 5.1, depending on the depth of Exchange-specific workflow integration.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The Suite Numérique de l'État: a case study in migration at scale

France's Suite Numérique, piloted by DINUM since its launch in May 2024, provides the most instructive available case study of a sovereign productivity migration at national scale. Its trajectory is worth examining without embellishment, because its successes and failures are equally informative.

The suite currently comprises six tools: Visio (video conferencing[1], based on LiveKit), Doc (collaborative note-taking), Fichiers (file storage, based on Nextcloud), Tchap (instant messaging, based on the Matrix protocol), Grist (no-code data management), and an AI assistant developed in partnership with Mistral AI[79]. All tools are hosted exclusively in France.

Adoption signals are mixed but directionally positive. Visio has exceeded 60,000 monthly users, with the French government having committed in January 2026 to migrate 2.5 million civil servants to Visio on nationally hosted infrastructure by 2027.[80] Tchap, made mandatory across ministries from September 2025, is reported to have reached between 300,000 and 375,000 monthly active users as of early 2026, up from approximately 100,000 in early 2022[81]. Grist has grown from 1,000 to 15,000 monthly users in one year. The AI assistant, tested by 10,000 agents, was scheduled for full deployment in early 2026 and should be well underway at the time of publication of this report.

These figures need to be read against the baseline. France has approximately 5.7 million public servants. Tchap's 375,000 active users represent roughly 6.5% of the public sector workforce, two years after mandatory deployment was ordered[82]. The Cour des comptes, in its July 2024 report on DINUM[83], delivered a verdict that the report does not soften: the Suite's tools have "excessive cost for low added value," adoption has never been broad despite significant investment, and DINUM suffers from "unstable strategy and limited interministerial adhesion." The court noted that the Prime Minister herself, in November 2023, directed ministers and cabinet members to use Olvid, a private alternative, rather than Tchap. That was an extraordinary signal from the head of government about confidence in her own administration's sovereign tool. DINUM's budget was cut from a peak of five times its 2019 level back to €79 million in commitment appropriations and €138 million in payment appropriations in 2023.

The Suite Numérique's trajectory establishes that sovereign migration cannot succeed through tool development alone. The Suite Numérique's technical foundation is sound. Its governance, change management, and interoperability are not yet adequate to drive adoption at the scale required. DINUM has itself identified interoperability between its tools as the next essential step. The lesson is structural: a sovereign productivity suite competes not only on features but on the seamlessness of the user experience, and users who are accustomed to the integration depth of Microsoft 365 will not migrate to a suite where the components do not yet talk to each other fluently. This is a solvable problem, and it is being solved, but it requires sustained investment and governance authority that the Cour des comptes found DINUM currently lacks.

The interoperability problem

1 France's earlier webconf.numerique.gouv.fr was Jitsi-based and is being decommissioned.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Migration at the individual organisation level is blocked not only internally but externally. A public administration that migrates to Nextcloud and Collabora Online still receives documents in .docx and .xlsx formats from partner administrations, citizens, contractors, and elected officials who remain on Microsoft platforms. Format compatibility has improved substantially (Collabora Online handles Microsoft Office formats at high fidelity for standard documents) but edge cases remain, particularly with complex Excel macros, advanced PowerPoint animations, and legacy VBA-dependent workflows. More fundamentally, Teams-based video meetings remain the de facto inter-organisational collaboration standard across European public and private sectors. An organisation that migrates internally to Visio must still join Teams calls with external partners. Here, the dependency is embedded in the inter-organisational fabric of European public administration, a collective action problem of exactly the kind described in section 1.3.

The same dynamic is illustrated by the DGFiP, which published a rigorous Linux workstation migration methodology in 2024 and yet deployed Windows 11 across its 95,000 workstations in 2025. The case is documented in full in section 6.4. Its relevance here is structural: methodological readiness cannot produce migration by itself without governance authority.

The French Ministry of National Education's procurement of March 2025 makes the same point at greater scale and with unusual internal contradiction. The ministry attributed a framework contract covering Microsoft solutions for central services and higher education establishments (minimum value €74 million, ceiling €152 million over four years, awarded to Crayon France) while simultaneously circulating a technical doctrine prohibiting schools from deploying non-sovereign digital solutions[84]. Deputy Philippe Latombe filed a formal written question requesting rescission on sovereignty grounds[85]. The Hexatrust association of French and European technology providers issued a public protest[86]. A concurrent Microsoft 365 migration at École Polytechnique, an institution under the Ministry of Armed Forces whose laboratories conduct research in defence and advanced technology, attracted parallel criticism on identical grounds[87].

What holds

An organisation fully migrated to Nextcloud and Collabora Online on European-hosted infrastructure retains internal operational continuity under commercial pressure: document creation, file storage, calendar, and messaging continue independently of any American platform decision. Email and file storage are the most resilient workloads post-migration. Video conferencing for external meetings is the most exposed residual dependency: an organisation that has migrated internally still joins Teams calls with every partner, ministry, and contractor that has not. The inter-organisational collaboration layer holds only as far as the least-migrated counterpart in the network.

What is missing

Two structural gaps are worth naming precisely. The first is a managed, enterprise-grade European productivity suite offering, i.e. the equivalent of what Microsoft 365 provides as a fully integrated, managed SaaS experience, but operated under European jurisdiction, with European-level support

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

SLAs, and without per-user pricing that becomes prohibitive at national scale. The technical components exist, but the integrated managed service layer on top of them does not yet exist at production scale for large public sector deployments.

The second is a coordinated migration demand signal. The organisations that have migrated successfully (Schleswig-Holstein, the Gendarmerie Nationale, the Austrian BMWET) share a common attribute that goes beyond the procurement decision: sustained political commitment at the leadership level. The organisations that have stalled (or at least migrated slower than expected), including France's broader public sector despite the Suite Numérique investment, have not had that sustained commitment translated into governance authority. No technical solution resolves a governance problem.

2.5 - Payments and financial transactions

Critical function: processing of financial transactions for public services with digital payment exposure: taxes, fines, fees, permits, public transport, subsidies. At the organisational level, payment infrastructure also covers supplier payments, payroll processing, and inter-administrative transfers.

Dominant U.S. actors: Visa, Mastercard, PayPal, Stripe.

Dependency level: CRITICAL (for public services with digital payment exposure)

The sanctions documented in the introduction to this report provide the most precisely documented illustration of how payment network dependency operates in practice. When U.S. sanctions were applied to ICC officials, Visa and Mastercard stopped working for the sanctioned individuals regardless of the country or bank that had issued their cards. The bank who issued the cards were not American, but since Visa and Mastercard operate as global clearing networks, every transaction, wherever it originates, is routed through their American-controlled authorisation infrastructure. The issuing bank is irrelevant: control sits upstream, at the network level.

Visa and Mastercard together process over €7 trillion in European payments annually and held approximately 61% of eurozone card transaction value in October 2025[88]. When PayPal and other American digital payment operators are included, the overwhelming majority of European digital payment flows through American-controlled infrastructure at some point in the transaction chain.

For European public organisations, this creates a specific operational exposure: any digital payment channel that routes through Visa, Mastercard, or PayPal infrastructure is, in principle, subject to American network-level decisions. This is a documented mechanism that has already been activated.

SEPA: the existing European rail and its limits

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The Single Euro Payments Area provides a European-controlled bank transfer infrastructure that does not route through American networks. SEPA credit transfers and direct debits are processed through European clearing houses (EBA Clearing, STET, and the Eurosystem's TARGET2) with no American intermediary. For bank-to-bank transfers, SEPA is a genuinely sovereign European rail.

Its limits are operational rather than jurisdictional. Standard SEPA transfers settle in one business day, which is unsuitable for real-time payment use cases. The SEPA Instant Credit Transfer scheme, which settles in under ten seconds, became mandatory for all eurozone banks by January 2025 under the Instant Payment Regulation[89]. As of early 2026, 88% of SEPA participants in the euro area are registered for instant payment, with many countries at 100% participation. This is a significant infrastructure development that is underweighted in most sovereignty discussions.

The gap SEPA does not address is the card payment and digital wallet layer. SEPA has no card scheme, no consumer-facing wallet. It processes bank transfers, not card transactions. The €7 trillion in annual card payments that Visa and Mastercard process in Europe have no SEPA equivalent. That is the structural gap that the European Payments Initiative is attempting to close.

The European Payments Initiative and Wero

The European Payments Initiative is a consortium of 16 major European banks (including BNP Paribas, Deutsche Bank, Société Générale, ING, and Worldline) backed by the European Commission, with €500 million in capitalisation. Its digital wallet, Wero, launched for peer-to-peer payments in Germany, France, and Belgium in 2024, with Luxembourg and the Netherlands set to join in 2026[90] and Austria shortly after[91]. It is built directly on SEPA Instant Credit Transfer infrastructure and as therefore bypasses card networks entirely: payments move account-to-account in under ten seconds, with no Visa or Mastercard in the chain.

By early 2026, Wero has over 47 million registered users[92]. E-commerce merchant payments went live in Germany in November 2025, with Lidl, Decathlon, and Rossmann among the first accepting merchants. France and Belgium follow in 2026. In February 2026, EPI signed a memorandum of understanding with the EuroPA Alliance (a coalition including Italy's Bancomat, Spain's Bizum, Portugal's MB WAY, and the Nordic Vipps MobilePay) to build a pan-European interoperable payment network covering 130 million users across 13 countries. The EU regulatory environment is supportive: the Apple NFC access ruling of July 2024 allows Wero to offer tap-to-pay on iPhones without routing through Apple Pay[93]. PSD3, expected in 2026, will further strengthen open banking requirements.

Wero is the most promising European payment sovereignty development in two decades. However, it is not yet a substitute for Visa and Mastercard at European scale. Several structural limitations remain. Coverage is currently limited to three countries, merchant acceptance outside Germany is nascent, and the physical card layer has been abandoned, limiting point-of-sale use cases in markets where contactless card payment is the dominant consumer behaviour. Participation remains restricted to 16 founding banks, creating a barrier to entry for merchants whose banks are not among them.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ECB President Christine Lagarde stated in early 2026[94] that Europe needs its own digital payment system urgently, and described the current situation (virtually all European card and mobile payments running through non-European infrastructure) as strategically unacceptable. The digital euro, targeted for 2029, would provide a central bank-backed complement to Wero, though its scope and design remain under discussion.

The structural over-compliance problem

The sanctions episode revealed a mechanism that extends beyond the targeted individuals themselves. European banks (whose cards were not American, whose clients were European) closed accounts and suspended services, not because they were legally required to do so under EU law, but because they feared secondary sanctions exposure from American regulators. This is structural over-compliance: European financial institutions pre-emptively applying American sanctions logic to their own client relationships, not because EU law mandates it, but because their correspondent banking relationships and dollar-clearing dependencies make American regulatory exposure a more immediate business risk than EU legal obligations. The result is that American sanctions reach extends well beyond its legal perimeter, amplified by European institutions acting in their own risk interest.

This mechanism is documented in the ICC case but not specific to it. The same logic drove European banks to exit Iranian correspondent relationships following the U.S. withdrawal from the JCPOA in 2018, despite the EU maintaining the agreement and activating the blocking statute. The EU Blocking Statute[95] (European Council Regulation 2271/96) prohibits European persons from complying with certain extraterritorial U.S. sanctions, and was updated in 2018 specifically to address the Iran situation. It has been largely ineffective[96] because the cost of non-compliance with American regulatory expectations consistently outweighs the cost of non-compliance with EU law, a structural asymmetry that no statute can resolve without addressing the underlying dollar-clearing dependency.

What holds

SEPA credit transfers and SEPA Instant (including Wero, which routes entirely over SEPA Instant rails) are structurally resilient to any scenario involving American platform pressure. No American corporate entity sits in the bank-to-bank transaction chain. Card-based transactions do not hold: any public service accepting Visa or Mastercard payments from citizens retains a dependency whose activation mechanism has already been documented in the introduction to this report. The asymmetry is immediate and actionable: organisations that redirect citizen payment channels toward SEPA-based instruments today reduce their exposure without waiting for Wero to reach full merchant coverage. This resilience holds at the network level. It does not extend to the application layer on mobile devices: a Wero transaction routed entirely over SEPA Instant rails still depends on Google Play Integrity to execute on Android terminals, a dependency that sits below the payment layer and is not addressed by any current European payment sovereignty initiative.

What is missing

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Three gaps are distinct and worth naming separately.

At the retail payment layer, Wero is closing the gap but has not yet closed it. Full pan-European merchant acceptance, point-of-sale NFC coverage, and integration of the broader EuroPA network are two to three years away on optimistic timelines. Until then, European public organisations accepting digital payments from citizens remain dependent on Visa and Mastercard for the majority of card-based transactions.

At the structural level, the over-compliance problem cannot be resolved by payment infrastructure alone. It requires reducing European banks' dependency on dollar-clearing and U.S. correspondent banking relationships, a process that is underway through the expansion of euro-denominated trade settlement and the Capital Markets Union, but that operates on a decade-long horizon, not a procurement cycle.

At the mobile application layer, a dependency sits below the payment network itself. Google Play Integrity is the proprietary attestation API through which Google determines whether payment, banking, and government applications are permitted to run on Android devices. The attestation is available exclusively for devices running Android with Google Play Services; alternative operating systems are structurally excluded from running these applications regardless of which payment network they connect to. In March 2026, a European consortium led by the German manufacturer Volla Systeme, and including the French custom ROM developer iodé and Murena, announced UnifiedAttestation: an open-source alternative to Google Play Integrity, intended for open-source release under a European foundation governance structure[97]. No operational deployment exists at the time of writing. The initiative is noted here because its architecture is instructive: open-source, European-led, governed by a European foundation, addressing a foundational infrastructure gap that no single market actor has a commercial incentive to close unilaterally.

2.6 - Content delivery, visibility and distribution

Critical function: this layer shapes two distinct vectors of public institutional exposure.

The first is strategic: search platforms and advertising infrastructure determine whether public services are visible to the citizens they serve, and web analytics platforms determine whether institutions can measure that visibility. Control over these functions is control over the conditions under which public information reaches the public.

The second is operational: content delivery networks, DDoS protection, and DNS resolution underpin the availability of every internet-facing service. Disruption here is immediate and visible. Dependency in this layer therefore operates on two timescales at once: analytical blindness accumulates slowly and silently, while infrastructure failure is acute and disruptive.

Both vectors are dominated by a small number of American operators.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Dominant U.S. actors: Cloudflare (CDN, DDoS protection, DNS), AWS CloudFront (CDN), Google (Search, Ad Manager), Meta (Ads).

Dependency level: SERIOUS

Rated SERIOUS rather than CRITICAL because failure at this layer degrades reach and resilience without halting operations. A public service that loses its CDN or DDoS protection does not immediately cease to function but becomes slower, more vulnerable, and potentially unreachable during attack conditions. If it loses search visibility, it keeps operating but become substantially harder to find.

The CDN and DDoS layer

Cloudflare operates the largest DDoS mitigation network by traffic volume, processing more attack traffic than any other single operator. In Q4 2025, Cloudflare's own threat intelligence reported mitigating 34.4 million network-layer attacks over the year, compared to 11.4 million in 2024.[98] Independent market analysis identifies Cloudflare alongside Akamai, Radware, Netscout, and Fortinet as one of five vendors that collectively account for the dominant share of global DDoS protection capacity.[99] No European operator appears in this group.

The dependency is not jurisdictional in the same way as cloud infrastructure: Cloudflare does not store data in the way a cloud provider does, and its role as a network intermediary creates a different risk profile than, say, Microsoft 365. The risk is of a different kind: Cloudflare sits in the traffic path between citizens and public services. It sees DNS queries, HTTP headers, and request metadata for every site it protects. In an adversarial scenario, that visibility is itself a form of dependency. The December 2025 Cloudflare outage, which impacted approximately 28% of all HTTP traffic it served for several hours[100], demonstrated the systemic fragility that comes with this degree of concentration in a single American-controlled network intermediary.

Existing EU alternatives for CDN and DDoS

Bunny.net (Slovenia) is the most credible European CDN alternative. It operates 119 points of presence globally, delivers an average latency of 24 milliseconds compared to Cloudflare's 28 milliseconds in independent benchmarks[101], and serves over one million websites. It is fully GDPR-compliant, EU-incorporated, and offers CDN, storage, DNS, video delivery, and basic DDoS protection. Pricing is transparent and competitive. It does not offer the breadth of Cloudflare's security suite (no Zero Trust, no full WAF at enterprise scale, no email security) but for core CDN and DNS functions it is a production-viable alternative that requires no architectural rethinking. Migration from Cloudflare to Bunny.net has been documented at taking under two hours for standard deployments[102].

Gcore (Luxembourg) provides CDN, DDoS protection, cloud, and edge computing with a European-majority infrastructure footprint and a more enterprise-oriented security offering than Bunny.net. Its DDoS protection capacity reaches 1.5 Tbps[103]. Used by European gaming, media, and public sector clients.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

KeyCDN (Switzerland) provides core CDN with European data centre focus, GDPR compliance, and straightforward pricing. Suitable for standard content delivery without advanced security requirements.

The honest gap: for high-volume DDoS mitigation against hyper-volumetric attacks (the kind that Cloudflare absorbed at scale in Q1 2025, blocking 20.5 million attacks including multiple exceeding 1 Tbps[104]) no European provider currently offers equivalent absorption capacity. Cloudflare's 358% year-on-year increase in blocked DDoS events in Q1 2025 illustrates the scale of the threat environment. For European public sector sites that are not high-value attack targets (i.e. the majority), Bunny.net and Gcore are adequate. For critical national infrastructure sites subject to nation-state-grade DDoS campaigns, the European alternative does not yet exist at equivalent scale.

This is in part a demand-side problem: DDoS absorption capacity scales with network infrastructure, which scales with customer volume and revenue. A coordinated European procurement signal that routes public sector CDN traffic toward European providers would directly increase their capacity to absorb the attacks that currently justify continued dependency on Cloudflare.

The search and advertising dependency

Google holds 91.4% of the European search engine market. In the European digital advertising market, Google and Meta together account for the dominant share of digital ad spend. For European public institutions, this creates a structural dependency on reach: the ability to communicate with citizens on terms the institution controls. A public health authority running a vaccination campaign, a tax administration directing citizens to file online, a municipality announcing a public consultation, all depend on Google and Meta for the distribution of that communication. Three decades of attempts to build a European search competitor have not changed this, and seeking to do so now would be misaligned with where information retrieval is actually moving.

Traditional keyword search is being progressively displaced by large language models. LLM-sourced web traffic grew 527% year-on-year between January and May 2025[105]. Google's global search market share fell below 90% for the first time since 2015 in Q4 2024[106]. Gartner forecasts a 25% reduction in traditional search query volume by 2026[107]. Among younger users, the shift is generational: 47% of Gen Z respondents reported weekly use of generative AI tools in a March 2025 Gallup survey[108], a figure that has nearly doubled year-on-year[109]. The strategic implication for public sector organisations is direct: the dependency that matters on a five-year planning horizon is not on Google Search, which is partially self-correcting as the technology layer shifts, but on the LLM infrastructure that is replacing it, documented in section 2.7, and concentrated at present in American platforms.

For the advertising and distribution layer, no individual procurement decision changes the reach equation. Two mechanisms operate at a level above the organisation.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The first is the DMA's obligations on Google as a designated gatekeeper, which require search result interoperability, data sharing with competing services, and prohibition of self-preferencing. The Commission opened proceedings in 2024 on Google's compliance with its search data sharing obligations. An enforced DMA obligation does not create a European search engine. It creates conditions under which European actors can build credible vertical search services for specific institutional domains, health, legal, administrative, on top of index data currently monopolised by Google. Enforcement is the variable to monitor, the designation itself changes nothing until it does.

The second is direct communication infrastructure: email lists, push notification systems, RSS feeds, and dedicated mobile applications that route institutional communication directly to citizens without any platform intermediary. These channels are within organisational reach, require no external dependency, and are systematically underinvested relative to paid channels that route budget to American platforms.

Web analytics: the most overlooked migration

Virtually every European public institution website transmits behavioural data (page views, session duration, user flows, referral sources) to Google in real time through Google Analytics, and to Meta through the Meta Pixel tracking script. The data transferred includes the navigation behaviour of citizens accessing public services, health information, legal and administrative content, and electoral information on government platforms. This represents a continuous, automated transfer of citizen behavioural data to American platforms, executed on every page load, from every public institution that has not explicitly disabled these scripts.

France’s CNIL ruled in 2022 that Google Analytics transfers constitute a violation of GDPR by routing personal data to U.S. servers subject to the CLOUD Act without adequate protection[110]. Austria's DPA reached the same conclusion. The European Data Protection Board's guidelines on transfers to third countries apply directly. The legal position is unambiguous.

European alternatives exist at production maturity and are deployed at scale across European public administrations. Matomo (Luxembourg, formerly Piwik) is the most widely deployed open-source web analytics platform in the world. It can be self-hosted entirely within an organisation's own infrastructure, processes no data outside the host environment, and provides the full analytics capability set required for institutional web governance. It is GDPR-compliant by architecture rather than by contractual warranty. A migration from Google Analytics to a self-hosted Matomo instance is technically straightforward, achievable within days for a standard institutional website, and has zero ongoing licence cost. Several European public administrations have completed this migration, and it does not appear in most sovereignty discussions because it is operationally unremarkable and simply done.

What holds

CDN and DNS functions hold well under pressure for organisations that have migrated to Bunny.net or Gcore: the traffic path between a public service and its citizens no longer passes through American-controlled infrastructure, and migration is achievable in hours for standard

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

deployments. DDoS protection at hyper-volumetric scale does not hold for high-value targets: no European provider currently offers absorption capacity equivalent to Cloudflare against nation-state-grade attacks. The search and advertising sub-layer holds nothing at the organisational level: no procurement decision changes the distribution economics of the European information environment. What holds there is determined by regulatory enforcement, not by anything an individual organisation can do.

What is missing

Two distinct gaps apply to two distinct problems in this layer.

For CDN and DDoS: the technical gap at the enterprise and hyper-volumetric level is real but narrowing and, as stated above, is a matter of critical mass for European actors which can be solved by reorienting public demand towards them. The more immediate gap is awareness: Bunny.net and Gcore are already genuinely viable for the majority of European public sector use cases and are not widely known or considered in procurement processes. This is partly the documentation problem identified in section 1.4.

For search and advertising: no procurement decision closes this gap. It requires either a European search engine reaching viable market share, which three decades of attempts have not produced, or a regulatory intervention that changes the distribution economics of the European information environment. The Digital Markets Act's designation of Google as a gatekeeper[111], and the obligations it imposes regarding search result interoperability and self-preferencing, is the most actionable current lever. Its enforcement is the relevant variable to monitor, not the procurement decisions of individual public organisations.

2.7 - Artificial intelligence and data processing

Critical function: language understanding, content generation, document analysis, decision support, and process automation across public sector workflows. Unlike previous layers, AI is not yet a baseline operational dependency for most European public organisations. It is an emerging one, being integrated at a pace that outstrips both governance frameworks and sovereignty assessments. The strategic importance of this layer lies less in what it currently enables than in what it is about to make irreversible.

Dominant U.S. actors: OpenAI (GPT-4o, o3, available via Microsoft Azure as the primary enterprise channel), Google Gemini (via Google Workspace and Vertex AI), AWS Bedrock (hosting Anthropic's Claude, Meta's Llama, and others), Anthropic (Claude, with Amazon as its largest investor at $4 billion committed).

Dependency level: EMERGING - but strategically critical

No other layer in this report carries a higher ratio of future risk to current visibility. The AI dependency being created in 2026 will be significantly harder to unwind in 2030 than the cloud dependency of 2015 is today. That is not a speculative claim, it follows directly from the integration pattern that cloud adoption produced: organisations that connected their workflows, data

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

architectures, and vendor relationships to AWS in 2012 spent the following decade discovering the depth of that commitment. AI integration is following the same pattern at higher speed and deeper integration depth. Sensitive public sector workflows (document drafting, citizen correspondence, legal analysis, benefits processing, procurement) are being connected to American LLM APIs faster than any governance framework can follow.

The investment asymmetry is stark and widening. In 2025, global AI venture capital reached $258.7 billion, with AI firms accounting for 61% of all venture capital worldwide, double the 2022 share.[112] U.S.-based firms attracted approximately $194 billion, or 75% of total global AI VC deal value. The EU27 attracted $15.8 billion, or 6%. The ratio has narrowed slightly from 2024 (when U.S. private AI investment reached $109.1 billion, 81% of the global total, against an estimated $3-4 billion for the EU27) because European AI investment grew substantially in absolute terms, driven in part by Mistral's fundraising.[113] The gap remains structural: the U.S. produced 40 notable AI models in 2024 against three from the EU27. The conditions that produced American cloud dominance are being reproduced, at greater speed, in AI.

Mistral AI: genuine strengths, current constraints

Mistral AI is Europe's most credible large language model provider and deserves an honest assessment, neither promotional nor dismissive.

Its strengths are real and documented. Founded in April 2023 by former Google DeepMind and Meta researchers, Mistral reached a valuation of €11.7 billion in September 2025 following a 1.7 billion euros investment round led by ASML[114]. Mistral's open-weight model strategy (through Mistral Large 3, Mistral Small 3.1 and Magistral reasoning models) directly addresses the sovereignty requirements that European public organisations cannot meet through proprietary American alternatives: organisations can self-host Mistral models on their own infrastructure, ensuring that no data leaves their perimeter. Mistral holds ISO 27001, ISO 27701, and SOC 2 Type II certifications. Its models are natively compliant with EU AI Act requirements. It has been awarded a framework agreement by France's Ministry of the Armed Forces for AI services deployed on French infrastructure, and a partnership with French civil service to equip 10,000 civil servants via its Le Chat assistant[115]. The French government's DINUM has integrated a Mistral-powered AI assistant into the Suite Numérique.

Its current constraints are equally real. While greatly increasing, Mistral’s current total revenue is negligible as a comparison to the operational scale of OpenAI or Google DeepMind[116]. Mistral's training infrastructure remains partially dependent on NVIDIA GPU clusters. Its most recent model family (as of the publication date of this report) was co-developed with NVIDIA on their latest GPU architectures. Mistral has since moved to address compute dependency directly through two infrastructure projects. The first, Mistral Compute, deploys 18,000 advanced AI chips in Essonne, France, announced in June 2025 and scheduled for operational deployment in 2026[117]. The second, announced in February 2026 in partnership with Swedish operator EcoDataCenter[118], is a €1.2 billion data centre investment in Sweden targeting operational capacity by 2027. Both represent a significant vertical integration effort. Neither resolves the underlying semiconductor dependency:

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

NVIDIA Grace Blackwell chips are American-designed, Taiwan-manufactured components, and Mistral's compute sovereignty is bounded by the same semiconductor supply chain constraints that apply to the European AI ecosystem as a whole, constraints the EU Chips Act targets but, according to the European Court of Auditors, is currently far off the pace to resolve by its 2030 deadline[119]. Microsoft holds a strategic investment in Mistral (€15 million convertible note from February 2024) and distributes Mistral Large models through Azure AI Studio, a distribution arrangement that extends Mistral's reach while embedding it in American cloud infrastructure for organisations that access it via Azure rather than self-hosted deployment. Analysts at Counterpoint Research assessed directly that Mistral's ability to "compete with general-purpose AI inference from hyperscale providers across enterprise and consumer markets seems unlikely at this point."[120] This is an honest assessment, not a dismissal: Mistral's strategic positioning is as a sovereign specialist, not a general-purpose hyperscaler challenger.

The InvestAI initiative, announced in February 2025 and operationalised through an amended EuroHPC regulation that entered into force in January 2026, provides a €20 billion facility to establish up to five AI “gigafactories” across the EU, each integrating over 100,000 advanced AI processors. These facilities are designed for the development and training of next-generation AI models at a scale that would represent a significant increase over current European capacity (the most powerful European AI supercomputer, JUPITER, operates approximately 24,000 AI accelerators) while remaining substantially below the largest American commercial AI infrastructure projects currently announced. [121] These facilities, if built on terms consistent with the sovereignty criteria documented in this report, would address the managed inference gap at a scale that no single member state programme has yet reached.

The managed inference gap

Organisations that want to use Mistral models without internal AI infrastructure have a clean sovereign option: Mistral's own API, operating under French jurisdiction, with contractual GDPR compliance, enterprise SLA tiers, and no use of submitted data for model training by default. The alternative, accessing the same Mistral models via Azure AI Studio, routes them through U.S. jurisdiction and CLOUD Act exposure.

The residual gap applies to a narrower profile: organisations whose data classification or sector regulations require that no data leave their own infrastructure perimeter, and that lack the internal engineering capacity to operate a self-hosted deployment. For that profile, no European operator currently provides a fully managed on-premises Mistral deployment as a standard procurable service. Organisations in that situation should self-host on European IaaS with external support, or flag the dependency under NIS2 Article 21 risk management obligations until the market closes the gap.

Other European AI actors

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Beyond Mistral, the European AI landscape includes actors worth noting for specific use cases. **Aleph Alpha** (Germany) specialises in explainable AI for regulated and government use cases, with Luminous models deployed in German federal agencies and the German armed forces[122]. **Ikomia** (France) and **LightOn** (France, now merged with Pleias) focus on enterprise and document AI. **Silo AI** (Finland, acquired by AMD in 2024[123] illustrating the ownership risk identified in the Solvinity discussion) produced strong multilingual Nordic-language models. The AMD acquisition removes Silo AI from the European sovereign ecosystem by the ownership test applied in this report. **NovaSky** and the broader open-source European model ecosystem building on Mistral's open-weight releases represent a diffuse but genuine capability base.

What holds

Self-hosted Mistral models on European cloud infrastructure are fully resilient to American platform decisions: no API suspension, no licence revocation, no CLOUD Act demand can reach a model running inside an organisation's own perimeter. That resilience is available today, for any new AI workload being onboarded. What does not hold is any workflow already integrated with an American LLM API. The integration depth increases with every passing month, and replacement becomes more costly with each cycle. The resilience differential in this layer is temporal rather than technical: the integration decision taken today determines the optionality available in two years.

What is missing

Three gaps are structural and interrelated.

The first is a managed, procurable European AI inference platform. Not just a model, but a full service stack including SLA, support, compliance documentation, audit trails, and contractual GDPR guarantees. An inference platform that a public sector procurement officer can sign without requiring an internal AI engineering team to make it work.

The second is compute independence. European AI capability ultimately depends on American semiconductor supply for training and, increasingly, inference. The EU Chips Act targets 20% of global semiconductor production by 2030, but the advanced GPU capacity required for frontier model training remains concentrated in NVIDIA and AMD, which are both American companies. This is a 10-year structural dependency, not a procurement decision.

The third is the governance gap. Sensitive public sector AI workflows are being connected to American APIs at a pace that procurement and GDPR compliance processes are not tracking. The AI Act's obligations for high-risk AI systems provide a framework[124], but enforcement is nascent and most public sector AI deployments in 2025 are not being formally assessed against high-risk classification criteria. The dependency is being created before the governance exists to assess it.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

2.8 - Software development and delivery infrastructure

Critical function: This layer is the operational backbone of any organisation that develops or maintains software which, in 2025, includes most European public administrations of any scale, either directly or through contractors whose delivery pipelines run on this infrastructure. This includes version control for source code, code review and collaboration workflows, continuous integration and delivery pipelines, and the package registries from which build dependencies are pulled.

Dominant U.S. actors: GitHub (Microsoft, acquired 2018), npm registry (GitHub/Microsoft, acquired 2020[125]), Docker Hub (Docker Inc.), PyPI (Python Software Foundation, U.S.-based), GitHub Actions (CI/CD).

Dependency level: SERIOUS

GitHub hosts over 1 billion repositories and is used by over 150 million developers worldwide[126]. As of Q4 2024, the European Union had surpassed the United States in cumulative git pushes on GitHub, the first time any economy or bloc had done so. The finding is drawn from GitHub's Innovation Graph dataset, which is openly downloadable and has been independently cited in peer-reviewed research linking open source contributions to economic output.[127]

The European Commission's own code, the Joint Research Centre's repositories, and the source code of numerous European public sector digital services are hosted on GitHub. In October 2024, GitHub introduced EU data residency for Enterprise Cloud customers[128], allowing code and repository data to be stored within the EU. The CLOUD Act exposure remains: Microsoft owns GitHub, and EU data residency does not resolve jurisdictional reach under U.S. law, as established in section 1.5 of this report.

The dependency is SERIOUS rather than CRITICAL because migration paths exist, are well-documented, and have been executed successfully at public sector scale. The blocker is not technical. It is organisational inertia and the network effects of a platform where the open-source ecosystem, external contributors, and upstream projects all converge.

The two-layer dependency structure

This layer contains two distinct dependency types that must be addressed separately.

The first is the **code hosting and collaboration layer**: where source code lives, where pull requests are reviewed, where issues are tracked, and where CI/CD pipelines are defined. This dependency is fully addressable through migration to self-hosted or European-hosted alternatives.

The second is the **package registry layer**: the upstream registries from which CI/CD pipelines pull dependencies at build time. An organisation that migrates its source code from GitHub to a self-hosted Forgejo instance still pulls JavaScript packages from npm[129], Python packages from PyPI, and container images from Docker Hub in every build. These registries are American-controlled infrastructure through which the software supply chain of every organisation building on standard open-source stacks passes by default. This dependency is not resolved by migrating the Git forge. It

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

requires a separate, deliberate intervention: either proxying registries through a European-hosted mirror, maintaining internal artifact repositories, or both.

Existing EU alternatives for code hosting

Three mature options exist for the code hosting layer.

GitLab (U.S.-incorporated but self-hostable; Community Edition is fully open source under MIT licence) is the most functionally complete self-hosted alternative to GitHub. It provides integrated source control, CI/CD pipelines, container registry, package registry, issue tracking, and security scanning in a single platform. It is deployed at scale in European public administrations including the German federal government's Open CoDE platform[130]. The ownership caveat is relevant: GitLab Inc. is a U.S. company, and self-hosted deployments of GitLab Community Edition use software developed under U.S. corporate governance. For organisations applying the ownership test strictly, this is a partial rather than full sovereignty solution, though it eliminates CLOUD Act exposure for data hosted on European infrastructure.

Forgejo (community-governed, non-profit, under Codeberg e.V., Germany) is a hard fork of Gitea developed under fully European non-profit governance. Licensed under the GNU General Public Licence since August 2024. It powers Codeberg, Germany's non-profit public code hosting platform. Forgejo is the strongest sovereignty story in this layer[131]: European governance, copyleft licence, non-profit structure, and active federation work that aims to enable cross-platform collaboration between independently operated code repositories, using the same open protocol that underpins federated social networks. Its constraint relative to GitLab is breadth: CI/CD via Forgejo Actions covers standard workflows but yet lacks GitLab's native security scanning depth and integrated DevSecOps tooling.

Gitea (open-source core, but trademark and domain controlled by for-profit Gitea Limited / CommitGo Inc., U.S.-incorporated at the time of writing of this report) occupies a middle ground. Functionally mature and widely deployed, but its governance trajectory since the 2022 incorporation of Gitea Limited has raised concerns that led to the Forgejo fork[132]. For organisations prioritising governance clarity, Forgejo is preferable.

For European public sector deployments, the practical choice is between GitLab Community Edition self-hosted (maximum feature breadth, U.S. corporate governance) and Forgejo self-hosted on European infrastructure (maximum governance sovereignty, adequate feature set for most public sector workflows).

CI/CD runners: the second layer of forge dependency. An organisation that migrates its source code from GitHub to a self-hosted Forgejo or GitLab CE instance retains a residual dependency if its CI/CD pipelines continue to run on GitHub Actions, whose runners execute on Microsoft-controlled infrastructure. Migrating the forge without migrating the runners resolves the code hosting exposure while leaving the build and deployment pipeline on American infrastructure. The remediation is the same self-hosted runner model: both platforms support deployment of the build execution environment on any European cloud infrastructure, removing the dependency on

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Microsoft-controlled servers for the compilation and testing of code. This configuration requires a dedicated infrastructure team to maintain and is better suited to organisations with that internal capacity. For smaller entities, a managed CI/CD offering on European infrastructure is the more realistic path.

The package registry gap

No European public registry exists for npm, PyPI, or Docker Hub at a scale comparable to the originals. Two distinct responses to this gap must be distinguished, as they differ in complexity, cost, and what they actually resolve.

The first is internal proxying. Any organisation can deploy an internal package cache (several mature open-source tools exist for this purpose) that stores local copies of software dependencies rather than pulling them from American-controlled registries at build time. This resolves the build-time dependency in disruption scenarios: a CI/CD pipeline pulling from an internal cache does not require live access to American-controlled infrastructure to complete a build. It also enables internal security scanning before packages enter the pipeline. Any organisation with internal IT capability can deploy an internal package cache within weeks and within normal operational budgets. What it does not resolve is the governance dimension: the upstream source of truth remains American-controlled, and the cache is only as current as its last successful synchronisation with that source.

The second response is the establishment of European sovereign registries with independent governance, maintained by European institutions, and capable of functioning as the primary publication point for open-source packages used in European public sector software. This is a fundamentally different undertaking. It requires a recognised governance structure (a foundation or consortium with the legitimacy to issue package identities and manage maintainer authentication), a security infrastructure for package signing and supply chain integrity, and sufficient adoption among maintainers to make dual-publication standard practice. The Rust ecosystem's crates.io, governed by the Rust Foundation, provides a reference model: a community-governed registry that functions as a credible alternative to centralised commercial infrastructure. Building an equivalent for npm or PyPI is a multi-year programme under the most favourable conditions. It is, however, structurally less constrained than semiconductor manufacturing or subsea cable governance: it requires institutional commitment and sustained funding over years rather than industrial infrastructure built over decades.

The supply chain security dimension compounds this exposure. The npm, PyPI, and Docker Hub registries have all experienced significant supply chain attacks in 2024 and 2025, including malicious code injected into widely used packages and backdoored container images that remained available for download for extended periods before detection[133]. These are not sovereignty risks in the jurisdictional sense but operational integrity risks that apply regardless of the nationality of the registry operator. An internal artifact proxy with scanning addresses both risk types simultaneously.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The caveat is that an artifact proxy's security value is bounded by the quality of its scanning. A self-hosted Nexus instance operated by a ten-person IT team will catch known vulnerabilities flagged in public databases. It will not detect a novel backdoor that the upstream registry itself has not yet identified. The organisational-level mitigation is real but partial. The structural answer is a European-operated registry with dedicated security resources, maintainer identity verification, and package signing infrastructure at a level that no individual organisation can replicate internally. That is a collective infrastructure investment, not a procurement decision, and it is the gap identified at the end of this section.

The strategic asymmetry

This section's most important observation is structural rather than technical. The source code of European public sector software (including code that implements citizen services, processes personal data, and manages critical infrastructure) is by default visible to American-controlled infrastructure. GitHub's terms of service permit Microsoft to access repository content for service operation purposes. GitHub Copilot, Microsoft's AI coding assistant, is trained in part on public repository content. The implications for public sector code that is inadvertently made public, or that is developed in private repositories on GitHub without EU data residency, are not theoretical. They are documented operational exposure at the layer where European public digital infrastructure is built.

What holds

Source code migrated to Forgejo or self-hosted GitLab CE on European infrastructure is resilient to GitHub access suspension: the codebase, its history, and the CI/CD pipeline continue to operate independently of any Microsoft decision. What does not hold is the build-time package registry dependency. A CI/CD pipeline pulling from npm, PyPI, and Docker Hub at build time retains three American-controlled dependencies regardless of where the source code is hosted. An internal artifact proxy with integrated security scanning resolves both the sovereignty exposure and the supply chain integrity risk simultaneously, and is achievable within normal operational budgets. The forge migration and the registry mitigation are two separate decisions, and the second is frequently overlooked by organisations that believe the first is sufficient.

What is missing

Three gaps are worth naming precisely.

The first is a managed, enterprise-grade European code collaboration platform: the equivalent of GitHub Enterprise, with full DevSecOps tooling, managed CI/CD runners on European infrastructure, integrated package registries, and the SLA and support model that public sector procurement requires. The technical components exist across GitLab CE, Forgejo, Nexus, and European cloud providers. The integrated managed service layer does not yet exist at production scale for large public sector organisations.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The second is awareness: the Open CoDE platform in Germany and France's code.gouv.fr demonstrate that European public code forges can be operated at national scale[134]. Neither is widely known outside its national context, and no EU-level equivalent exists.

A third gap is emerging and deserves explicit mention: AI coding assistants integrated into development pipelines. GitHub Copilot, the dominant product in this category, is deployed directly within developer IDEs and has access to the code being written in real time. For public sector development teams working on source code that implements citizen services, processes personal data, or manages administrative workflows, Copilot transmits the code currently being written, along with surrounding file content and repository context, to Microsoft's infrastructure with each completion request. Enterprise plans can be configured to disable prompt retention for model training, however the transmission itself, and the jurisdictional reach it creates under the CLOUD Act, is not configurable out.[135] This is a dependency that does not appear in any standard IT asset inventory and is not resolved by migrating the source code repository. European alternatives exist and are deployable today: Continue.dev is an open-source IDE extension that routes completion requests to any configured LLM backend, including self-hosted Mistral models on European cloud infrastructure. Tabby is an open-source, self-hosted coding assistant with equivalent IDE integration. Both require the self-hosted inference infrastructure documented in section 2.7 as a prerequisite. The dependency is named here because it is being created at speed, is invisible to most IT governance processes, and is resolved by the same architectural decision (self-hosted inference on European infrastructure) that addresses the broader AI dependency.

Section 3 - What failure looks like: disruption scenarios

A dependency map without a resilience map is half an assessment. The layers described in section 2 do not all fail in the same way, at the same speed, or under the same conditions. Some hold without any prior preparation. Some hold only if a decision has already been taken. Some do not hold at all, under any scenario, and the honest response to that is documentation and sequencing rather than denial.

The three scenarios that follow are ordered by likelihood, not by severity. They structured stress tests, each designed to answer a specific operational question: what breaks first, what can be switched under pressure, and what requires years of prior work to be resilient at all. A decision-maker who can answer those three questions for their own organisation's stack has what this section is intended to produce.

3.1 - Political pressure without technical disruption

Likelihood: high. Time horizon: immediate.

This is the scenario most closely approximated by the sanctions episode documented in the introduction: no system was taken offline, no contract was formally terminated, but access to

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

operational tools was interrupted for individuals acting in an institutional capacity. No system is taken offline, no contract is formally terminated. The pressure operates through the licensing and network dependency layer: American platforms continue to function for everyone except the targeted organisation or individual, which is what makes the mechanism effective. The technical infrastructure is intact, but the access is not.

The services that fail under this scenario are not those with the weakest technical foundations. They are those whose operational continuity is contingent on a decision made outside the organisation's legal perimeter.

Microsoft Entra ID is the most exposed single point. Licence suspension does not require a cyberattack, a service outage, or a contractual dispute. It requires an instruction to a U.S.-incorporated company. Any organisation whose identity infrastructure runs exclusively on Entra ID loses authenticated access to every connected system simultaneously: email, file storage, internal applications, VPN, developer pipelines. The failure is invisible in normal operations until it is in effect, at which point it becomes total and instantaneous.

Microsoft Teams inter-organisational dependency fails through a different mechanism. Even an organisation that has fully migrated its internal collaboration infrastructure retains a network-level dependency: its counterparts (ministries, contractors, partner institutions) have not migrated. Under political pressure, the targeted organisation is not denied access to Teams. It is denied the ability to collaborate with every organisation that remains on it. The dependency structure is the same documented in sections 2.2 and 2.4: the targeted organisation retains access to the tool but loses access to the network that has formed around it.

International card payment infrastructure fails by the mechanism documented in the introduction. Visa and Mastercard authorisation runs through American-controlled clearing networks regardless of the nationality of the issuing bank. Suspension does not require action by the cardholder's bank but only at the network level, upstream of every European financial institution in the chain. The ICC case, documented in the introduction, established that this mechanism operates within days of a political decision and affects cardholders regardless of their country of residence.

SEPA credit transfers and SEPA Instant, including Wero transactions, hold structurally under this scenario for the reasons established in section 2.5: no American entity sits in the clearing chain, and no political decision in Washington reaches a payment initiated between two eurozone accounts.

Bare-metal IaaS at European providers with no American shareholders (OVHcloud, Hetzner, STACKIT) operates under contracts governed by European law, on infrastructure located in European data centres, with no licensing dependency on American platforms. A virtual machine running in a French data centre under a contract with a French entity cannot be switched off by an instruction to a U.S.-incorporated company, because no such company is in the contractual or operational chain.

A sovereign EDR already deployed (HarfangLab, Tehtris) continues to detect and respond to threats independently of any American vendor decision. Detection capability does not depend on American

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

platform availability, licence renewal, or telemetry routing. The irreducible OS-layer dependency on Microsoft's kernel architecture applies here as it does universally, but it does not affect the operational continuity of the detection function under a political pressure scenario.

Political pressure without technical disruption is the scenario that most rewards prior preparation and most punishes the assumption that dependencies that have not yet been activated will never be.

3.2 - Targeted commercial suspension

Likelihood: low but non-zero. Time horizon: days to weeks.

This scenario is qualitatively different from the preceding one. Political pressure operates through licensing and network dependencies while leaving technical infrastructure intact. Commercial suspension removes the infrastructure itself. An organisation whose cloud workloads run on AWS, whose identity provider is Entra ID, and whose collaboration suite is Microsoft 365 does not experience degradation. It experiences cessation across all three layers, simultaneously, with no fallback that has not been prepared in advance.

The Huawei case is the most precisely documented precedent for how fast this mechanism operates in practice. In May 2019, the U.S. Department of Commerce added Huawei to the Entity List [136]. Within 24 hours, Google had suspended Huawei's Android licence, cutting off access to the Play Store, Gmail, Google Maps, and future Android security updates for all new devices [137]. Within days, Qualcomm, Intel, Broadcom, and ARM had announced they would cease supplying components[138]. Huawei was the world's second-largest smartphone manufacturer. It had been building on American technology for over a decade. The commercial suspension was not phased, not negotiated, and not anticipated in the company's operational planning. What the Huawei case established, and what is directly relevant to any European organisation building on American platforms, is the speed and totality of the mechanism: a single administrative decision, executed through the licensing relationships of U.S.-incorporated companies, can sever an organisation's access to its operational infrastructure within a working day.

The operationally significant variable in this scenario is therefore not which layers fail. It is which layers can be switched, at what speed, and under what prior conditions. Those three questions have different answers, and conflating them produces a resilience assessment that is neither honest nor useful.

What can be switched within 72 hours, without prior preparation

CDN and DNS routing to a European provider is documented as achievable in under two hours for standard deployments. Bunny.net migration from Cloudflare requires a DNS record change and propagation time. No data migration, no architectural rethinking, no prior contract. The dependency is real and the switching cost is negligible.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

SEPA-based payment channels hold by construction, as established in 3.1. An organisation that has already directed citizen payment flows toward SEPA instruments before a suspension event has no payment continuity exposure at this layer. An organisation that has not has no 72-hour remediation path for its card payment dependency: Visa and Mastercard acceptance cannot be replaced at speed.

A messaging platform deployed under crisis conditions can be operational in days, but user adoption, established communication channels, and the trust that comes from routine use cannot be manufactured at speed. The organisations that maintained communication continuity under the scenarios documented in section 3 were those whose users already knew where to go.

What can be switched within 30 days, with prior contractual preparation

Cloud IaaS migration to OVHcloud, Hetzner, or STACKIT is achievable within weeks for core workloads (compute, storage, managed Kubernetes) if two prior conditions are met: the alternative provider has been pre-contracted, and the workload architecture does not depend on platform-specific managed services that have no European equivalent. An organisation that has pre-contracted European IaaS as a secondary environment and maintains infrastructure-as-code deployable against a provider-agnostic API is in a materially different position from one that has not. The constraint is the prior decision to prepare, not the migration itself.

HarfangLab can be deployed in parallel with an existing American EDR on the same endpoints, allowing a transition without a detection gap. The prior condition is a procurement decision and a deployment test on a pilot population. Neither requires exceptional budget or political commitment, but they do require that the decision has been taken before the event.

What does not hold without structural preparation

IAM is the most operationally critical failure under this scenario and the hardest to remediate under pressure. An organisation whose identity infrastructure runs exclusively on Entra ID, and which has not deployed a parallel Keycloak environment with replicated user directory and federation configuration, loses authenticated access to every connected system at the moment of suspension. There is no 72-hour or even 30-day remediation path. A Keycloak migration at production scale, with high-availability clustering, directory synchronisation, application re-integration, and user training, is a months-long programme under calm conditions. It cannot be compressed into a crisis.

Business applications with deep Azure AD integration compound this exposure. Enterprise resource planning systems, HR platforms, case management tools, and sector-specific applications that authenticate exclusively through Entra ID do not fail independently of the IAM layer, they fail with it. The application continuity problem is not separable from the identity problem. An organisation that has audited its application portfolio for Entra ID integration depth before a suspension event knows exactly what fails and in what sequence. An organisation that has not is discovering its dependency in real time, under operational pressure, without the information needed to triage.

The productivity suite layer (Microsoft 365 in full suspension) is severe but more tractable than IAM for one specific reason: document creation and file access can be degraded gracefully. Local copies of documents remain accessible. A pre-deployed Nextcloud instance with replicated file

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

content provides continuity for the file storage function. What does not hold is real-time collaborative editing, calendar synchronisation across the organisation, and Teams-based communication with every external counterpart simultaneously. These are significant operational constraints but not existential ones for an organisation with any prior preparation.

What the Huawei precedent establishes

The Huawei precedent is instructive not only for its speed but for what it revealed about preparation. Huawei's founder had publicly acknowledged the risk years before the embargo, had invested in component stockpiling, and had begun development of an alternative operating system as a contingency[139]. None of that preparation was sufficient to prevent severe disruption to its smartphone business, because the architectural dependency on Google's proprietary services (the Play Store, the app ecosystem, the certification programme) had been built over a decade and could not be unwound in weeks. Huawei's preparation failed not because it was insufficient in volume but because it addressed components rather than architecture.

The distribution of outcomes in this scenario is binary in a way that the political pressure scenario is not. Under political pressure, an unprepared organisation experiences degradation. Under commercial suspension, an unprepared organisation experiences cessation at the layers that matter most. The difference between an organisation that has pre-contracted European IaaS, pre-deployed Keycloak alongside Entra ID, and redirected payment flows to SEPA instruments, and one that has not, is not a difference of degree. It is a difference in whether the organisation continues to function.

None of the preparations described above require a migration to be complete before they provide value. A parallel Keycloak deployment that covers 20% of applications is 20% of the IAM exposure resolved. A pre-contracted OVHcloud environment with no live workloads is a fallback that can absorb traffic within hours. The asymmetry between the cost of preparation and the cost of unpreparedness under this scenario is the central argument for the prioritisation logic developed in section 5.

3.3 - Full rupture

Likelihood: very low. Function: limit scenario.

Again, this scenario is not a forecast but a stress test applied to the dependency map for a specific analytical purpose: to identify the dependencies that no procurement decision, no migration programme, and no national policy can resolve within a five to ten year horizon. These are the irreducible constraints, the ones that define the outer boundary of European digital autonomy regardless of what happens at every other layer.

The scenario assumes a complete and sustained rupture of transatlantic technology relationships: American platform services unavailable, American semiconductor supply restricted, American-controlled internet infrastructure no longer operating under cooperative norms. The probability is low enough that planning for it as an operational scenario would be disproportionate for most

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

organisations. Its diagnostic purpose is to locate the ceiling of European digital autonomy regardless of what happens at every other layer.

The irreducible dependencies

Semiconductor supply is the most structurally constrained layer in this scenario. Frontier AI model training and inference depend on NVIDIA and AMD GPU architectures, both American-designed, the majority manufactured at TSMC in Taiwan. European cloud providers run their GPU capacity on the same hardware. Mistral's compute infrastructure, as documented in section 2.7, is built on NVIDIA Grace Blackwell chips. This dependency cannot be solved within a procurement cycle or a parliamentary term. It is a structural constraint on the upper bound of European AI and high-performance computing sovereignty for the next decade, regardless of what happens at the software and services layer.

Transatlantic physical infrastructure presents a different category of irreducibility. Submarine communication cables carry approximately 95% of international data traffic. As noted in the methodological section of this report, the United States maintains a consolidated licensing and oversight regime for submarine cables through the FCC, while the European Union has no institutional equivalent at Union level, as documented in a European Union Agency for Cybersecurity (ENISA) 2023 report[140]. In a full rupture scenario, the physical layer of transatlantic connectivity operates under governance asymmetry that no European organisation can resolve unilaterally. The gap is institutional, not technical, and it sits outside the decision space of individual organisations or even member states.

The software package registry layer (npm, PyPI, Docker Hub) represents a dependency whose depth is routinely underestimated because it is invisible in normal operations. As documented in section 2.8, every organisation building on standard open-source stacks pulls build dependencies from American-controlled registries at compile time. In a full rupture scenario, these registries become unavailable or unreliable simultaneously. Organisations with internal artifact proxies and offline mirrors are resilient. Organisations without them discover, at the moment their CI/CD pipelines fail, that their software supply chain has a dependency they never explicitly contracted for and never explicitly assessed.

What holds structurally

A property of European digital infrastructure that emerges under this scenario, though not under the more likely ones examined in sections 3.1 and 3.2, is that its structural heterogeneity reduces single-point-of-failure exposure relative to concentrated hyperscale architecture. This is a property the European landscape possesses by default rather than by design, and it functions as a resilience asset only under conditions where the coordination costs it also imposes are not the binding constraint.

American hyperscale architecture is optimised for efficiency through concentration. Three providers hold approximately 70% of the European cloud market. A single CDN intermediary carries 20% of global web traffic. A single identity provider is bundled into the productivity suite of the majority of European public administrations. These concentrations produce cost and performance advantages

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

under normal operating conditions. Under a full rupture scenario, they produce single points of failure at continental scale. The July 2024 CrowdStrike incident, a single configuration file update halting 8.5 million systems simultaneously, demonstrated this property under conditions far short of a full rupture scenario.

European digital infrastructure, by contrast, is fragmented across dozens of providers, national platforms, and open-source deployments operating under different jurisdictions, different governance structures, and different technical architectures. This fragmentation is the characteristic most frequently cited as a competitive weakness relative to American hyperscalers. Under a full rupture scenario, it is a resilience asset: there is no single point of failure, no single jurisdiction, and no single point of political leverage. A disruption that takes down AWS in one decision takes down a fraction of European infrastructure in the same decision, because the rest of it was never connected to the same switch.

This property is not a reason for complacency, and it is not available under the more likely scenarios examined in sections 3.1 and 3.2, where the absence of coordinated response capacity is the binding constraint rather than the absence of architectural diversity. What the full rupture scenario reveals is narrower: that the distributed structure of European digital infrastructure, a product of fragmentation rather than of deliberate resilience engineering, does reduce single-point-of-failure exposure in ways that concentrated hyperscale architecture does not. That property erodes with every consolidation decision. The policy implication is not to celebrate fragmentation but to preserve architectural diversity while building the coordination layer, documented in section 4, that would make it function as a deliberate resilience instrument rather than an accidental one.

The five to ten year boundary, and what moves it

Three dependencies identified in this scenario differ sharply in their tractability. Only one is immediately addressable at political will. That assessment should be read as a specification of what the required action looks like and at what level it must be taken rather than a justification for passivity.

The open-source package registry layer is the most tractable of the three, but it requires the same distinction drawn in section 2.8 between two responses of different scope. At the organisational level, internal artifact proxies resolve the build-time resilience problem within normal operational budgets and in a matter of weeks: this is merely a short term operational decision. At the systemic level, establishing European sovereign registries with independent governance, capable of functioning as primary publication infrastructure rather than downstream caches, is a multi-year programme. It is less constrained than the semiconductor and physical infrastructure dependencies described below, as it does not require industrial manufacturing capacity or physical deployment at sea. It does require institutional legitimacy, a recognised governance structure, and sufficient engagement from the open-source maintainer community to make dual-publication viable. Those conditions are achievable within a three-to-five year horizon with adequate political commitment,

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

and the distinction between this and the decade-long horizon of semiconductor sovereignty matters for sequencing the policy agenda.

Semiconductor supply is the most structurally constrained dependency. That being said, there are two industrial trends or trajectories that are worth tracking explicitly.

The first is European. The EU Chips Act targets 20% of global semiconductor production by 2030, though as noted in section 2.7, the programme is currently off pace to meet that target. The gap between ambition and execution is real but the infrastructure investments being made by TSMC in Dresden and Intel in Magdeburg represent the first serious European advanced semiconductor manufacturing capacity in a generation. These facilities will not produce frontier GPU architectures by 2030, but that is not their aim. They will establish the industrial foundation on which a more credible European semiconductor trajectory can be built in the decade that follows.

The second trajectory of interest is Chinese. Following sustained American export controls on advanced GPUs and TPUs (the chips that AI workloads run on), China has accelerated domestic semiconductor development at a pace and scale that was not widely anticipated. Huawei's Ascend 910B and 910C series, and the broader ecosystem developing around them, are not currently equivalent to NVIDIA's Hopper or Blackwell architectures in raw performance. They are, however, also not standing still. The software ecosystem compatibility gap (NVIDIA's CUDA remains the dominant programming model for AI workloads) is a real constraint today. At a ten-year horizon, the combination of Chinese state investment, forced decoupling from American supply chains, and the incentive structure of a trillion-dollar AI market makes it unlikely that gap will remain where it is. For European organisations and policymakers, the relevant observation is not whether Chinese semiconductor alternatives are preferable to American ones, but rather the fact that an alternative seems to be emerging at all. On current evidence, a more competitive multi-polar semiconductor landscape at the ten-year horizon is more likely than the continuation of the current duopoly. Monitoring Chinese semiconductor development as a strategic variable therefore appears operationally relevant.

For transatlantic physical infrastructure, the governance asymmetry documented above is real but not immutable. European operators are active participants in the subsea cable ecosystem: Orange Marine is among the leading global cable deployment and repair operators, and European telecoms groups collectively hold significant ownership stakes in transatlantic cable systems. The institutional gap lies is at the regulatory and coordination level. The NIS2 Directive already establishes a framework for critical infrastructure coordination across member states, and its extension to submarine cable governance is a natural and achievable next step. Neither the technical capacity nor the institutional architecture needs to be built from scratch.

Though they pose significant challenges, each of these constraints has a trajectory that current investment and policy decisions can accelerate. None is permanent.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Section 4 - The European levers: from diagnosis to action

The organisations described in section 2 are not waiting for permission to build. OVHcloud, HarfangLab, Nextcloud, Mistral, and Wero exist, operate at production scale, and have in several cases already demonstrated that the alternative is viable. The missing variable for widespread adoption is the ecosystem: certification frameworks, interoperability standards, procurement architecture, and the structural incentives that would allow these products to be selected at scale, maintained over time, and interconnected in ways that match the operational reality of European public institutions.

The levers described in this section address that ecosystem. This list should not be seen as a catalogue of options from which decision-makers should select according to preference, but rather as a structured and partially ordered path.

Some levers are normative prerequisites: the certification frameworks, protocol standards, and portability floors that define what sovereignty means in contractual terms, so that procurement decisions have something to land on (sections 4.1, 4.2, 4.3).

Others aggregate demand: the joint procurement architecture and member state coordination that convert fragmented national decisions into a market signal large enough to anchor investment cycles at European providers (sections 4.4 and 4.5).

A third group can be activated immediately and in parallel with all of the above: the governance and communication mechanisms of section 4.6, and several of the proactive instruments of section 4.7, do not wait for certification frameworks to be finalised or procurement catalogues to be built. The International Procurement Instrument can be signalled now, antitrust enforcement is already operational and the lobbying correction fund can be launched under existing budget lines. These instruments derive additional credibility from the normative and demand-side work of the preceding sections, but they do not require it as a precondition.

The one genuine sequencing dependency is between the normative layer and demand aggregation: a joint procurement framework built before certification standards exist has no eligibility criteria to enforce and reproduces the fragmentation it is designed to address. Everything else can proceed in parallel, and should.

The section concludes with section 4.7, which documents the shift from defensive posture to structural initiative. Several of its instruments are among the most immediately actionable in this section. They are placed last not because they come last, but because they are most legible once the defensive logic of the preceding sections has been established.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

4.1 - The regulatory lever: sovereignty criteria through sectoral mandates and the CADA

The European Union Cybersecurity Certification Scheme for Cloud Services (EUCS), developed by ENISA under the Cybersecurity Act, was designed to give public sector buyers a reliable, harmonised signal about the sovereignty properties of cloud services. Early drafts included explicit immunity requirements conditioning the highest certification level on EU corporate structure and absence of extraterritorial legal exposure. Those requirements were progressively removed. In March 2024, the level requiring EU majority ownership and immunity from non-European legal jurisdiction was deleted from the scheme. This outcome followed a documented lobbying campaign by a coalition of organisations representing the American technology industry (ITI, AmCham EU, BSA, and CCIA Europe) whose public submissions to the EU consultation process called explicitly for the removal of these criteria.[141] [142] The Commission relaunched the EUCS in January 2026 in a revised framework that separates technical certification from sovereignty questions[143], with a companion instrument, the Cloud Access for Data Act (CADA), intended to address the sovereignty dimension that the EUCS can no longer carry politically.[144]

The battle over the EUCS illustrates a structural dynamic that decision-makers must account for: the alignment of certain member state economic interests with those of American hyperscalers at the standards-setting level. Enterprises in member states with deep operational dependencies on American platforms have an immediate economic interest in avoiding sovereignty thresholds that would impose transition costs. That interest is short-term and diametrically opposed to medium-term strategic (and, as the cases documented in this report seem to indicate, economic) interests, but it exists still. The Solvinity case in the Netherlands, where a critical citizen authentication infrastructure nearly passed under American corporate control through a routine acquisition, illustrates what the absence of sovereignty criteria produces in practice. The argument for sovereignty thresholds is strongest precisely where its opposition is most organised.

Four levers are available to decision-makers who accept this diagnosis.

The first is sectoral mandate as substitute for EUCS. SecNumCloud in France, C5 in Germany, and ENS in Spain already function as sovereignty-grade certification frameworks. Embedding them (or a jointly developed framework derived from them, at the EU scale) as mandatory eligibility conditions in sectoral regulations (NIS2 implementing acts, the data governance framework for health data, DORA technical standards) creates procurement floors that operate independently of whether the EUCS carries sovereignty criteria. This is what France has done with its national cloud doctrine for sensitive workloads. Extending this logic through bilateral or multi-lateral coordination, then to willing coalitions of member states, creates a *fait accompli* that a sovereignty-neutral EUCS cannot undo.

The second is the CADA as the operative sovereignty instrument. If the CADA is designed with binding legal effects (e.g. conditioning access to public sector markets for sensitive workloads on demonstrable immunity from extraterritorial legal reach) it becomes the instrument the EUCS failed to be. The critical variable is whether the CADA will carry eligibility thresholds or optional

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

certification criteria. Decision-makers should monitor the CADA legislative process and engage at the member state level to ensure it carries binding eligibility thresholds rather than recommendations.

The third is coalition of exposed member states. The Baltic states, Poland, Finland following the SUPO assessment on election data, the Netherlands following the Solvinity case, and France have convergent positions on digital sovereignty that several other member states do not yet openly share. A coalition of five to seven member states adopting aligned sovereignty criteria in national regulations creates pressure on the EUCS and the CADA from the outside, independent of the consensus dynamics that have stalled European-level instruments.

The fourth is making the medium-term German interest explicit. Germany's short-term economic interests in avoiding sovereignty thresholds are real but diverge from its medium-term strategic exposure. German enterprises dependent on American cloud infrastructure face the same acquisition and jurisdictional risks documented throughout this report. The Solvinity case is the argument: Dutch infrastructure operators believed they had achieved sovereignty through a European provider, and then the provider was acquired by an American company. The same dynamic applies to any European enterprise or public body whose sovereignty assessment stops at the provider's current ownership and does not account for future acquisition risk. That argument is most persuasive when made by German counterparts to German decision-makers, which is why the Franco-German digital sovereignty commitments of November 2025 matter beyond their immediate policy content.

The U.S. FedRAMP model is an operational reference for what a pre-qualification catalogue with binding effects looks like at maturity: a single assessment, reused across agencies, creating a pre-qualified catalogue from which procurement can draw without per-agency duplication. Whether that model is adapted through a reformed EUCS, the CADA, any other European legislative vehicle or even national sectoral mandates is a secondary question. The primary question is whether sovereignty criteria function as eligibility thresholds or as optional scoring factors. That distinction is the one decision-makers should monitor in every instrument that emerges from the current legislative cycle.

4.2 - The standards lever: mandate open protocols where the Interoperable Europe Act already provides the vehicle

The Interoperable Europe Act, which entered into force in April 2024, requires mandatory interoperability assessments for all public sector bodies, including EU institutions, bodies, and agencies. The Interoperable Europe Board held its first meeting in December 2024 and adopted the first official guidelines on interoperability assessments. Interoperability assessments became mandatory as of January 2025.

This is an operational institution with a legal mandate. Its current scope covers general cross-border interoperability of public digital services. The gap this report identifies is specific: the Act does not

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

yet address the collaboration and identity federation layers where the dependency documented in section 2 is most acute and where a shared open protocol standard would most directly reduce switching costs.

Three interventions, each within the existing mandate of the Interoperable Europe Board, would materially change the landscape.

The first concerns messaging and collaboration. The Matrix open protocol is already deployed as the operational standard for secure instant messaging in multiple European public administrations: France's Tchap, Germany's Bundeswehr messaging platform[145] [146], and several other national deployments. A Board recommendation mandating Matrix-compatible endpoints for inter-organisational public sector communication would not require any organisation to replace its internal platform. It would require that whatever internal platform is operated exposes a Matrix-compatible federation endpoint, the same logic by which email interoperability operates across providers. The instrument is a standards mandate, and its effect is to prevent any single platform from holding inter-organisational communication as a captive network.

The second concerns document formats. The Open Document Format (ODF) is already an ISO standard and is already mandated for public sector document exchange in several member states. A Board recommendation extending ODF mandate to all cross-border document exchange between EU public sector bodies, combined with a requirement that public sector procurement processes accept ODF as the default submission format, removes one of the most persistent friction points in the productivity suite migration documented in section 2.4.

The third, and most structurally significant, concerns B2B identity federation. The eIDAS 2.0 regulation and the European Digital Identity Wallet are moving toward a citizen-facing authentication standard. The equivalent for machine-to-machine and administrative B2B authentication does not yet exist at European scale. The Interoperable Europe Board is the natural institutional home for a mandate requiring that all European public administrations expose an OpenID Connect-compatible federation endpoint, the mechanism by which one organisation's identity infrastructure can authenticate users from another without either organisation depending on a third-party commercial identity provider. This resolves, at the standards layer, the B2B federation problem identified in section 2.2 as the most structurally complex residual IAM dependency.

The precedent for what a well-designed European interoperability standard can achieve at market scale is not theoretical. GSM was a European standard that reshaped the global telecommunications industry. SEPA is a European payments standard that created a genuinely sovereign European rail for bank transfers where none existed. Neither required a European competitor to the incumbents it displaced. Both required a regulatory decision to mandate an open protocol and an institutional commitment to enforce it.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

4.3 - The DC-EDIC mandate: workload portability without architectural convergence

The Digital Commons EDIC, established by Commission decision in October 2025 and launched in December 2025 with France, Germany, the Netherlands, and Italy as founding members, is the most structurally serious European digital sovereignty instrument created since Gaia-X, and the one most deliberately designed to avoid its predecessor's governance failure. Its statutory mandate to develop and operate cross-border open-source digital infrastructure, combined with the explicit exclusion of commercial hyperscalers from its governance structure, gives it the institutional conditions that Gaia-X lacked.

The risk it faces is different from Gaia-X's governance capture risk. It is the risk of architectural overreach: attempting to define a common European cloud or AI architecture that resolves the interoperability problem by replacing provider diversity with a single European standard. That path trades one form of concentration for another. The resilience of European digital infrastructure under full-rupture conditions, documented in section 3.3, is a product of architectural heterogeneity. A single European technical standard, however well-designed, would progressively erode the property that makes European infrastructure more resilient to single-point disruption than American hyperscale architecture.

The productive mandate for the DC-EDIC is therefore more specific. It should define, by layer, a minimum portability floor below which no provider accessing European public sector procurement can fall, while leaving providers free to differentiate above it. The floor does not prescribe a common architecture. It prescribes the minimum that any organisation must be able to do: move its workloads, data, and identity infrastructure from one European provider to another within a documented process and timeline, without losing data and without rebuilding application architecture.

At the cloud infrastructure layer, the portability floor requires three things: virtual machine image export in an open format, object storage accessible via a documented API, and managed container orchestration deployable from provider-agnostic configuration files. These correspond to existing open standards that most European providers already support. Making them a condition of public sector procurement eligibility converts a voluntary feature into a market requirement without mandating a common technical architecture.

At the identity layer, the portability floor requires that any public sector IAM solution expose OpenID Connect and SAML 2.0 federation endpoints. This does not mandate any specific product. It mandates the protocol surface that allows one organisation's identity infrastructure to authenticate users from another's without either depending on a third-party commercial provider. The mechanism is identical to email interoperability: providers differ in architecture and pricing but they cannot differ in their ability to federate on the standard protocol.

At the collaboration layer, ODF as the default document exchange format for inter-administrative communication, and Matrix-compatible federation endpoints for inter-organisational messaging,

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

follow the same logic. An administration is not required to use LibreOffice or any specific platform. It is required to use software that produces and consumes the open standard.

At the AI inference layer, the portability principle translates differently. Workload portability in AI terms means the ability to switch inference providers without retraining proprietary-format models or rebuilding API integrations from scratch. The portability floor for AI workloads procured for sensitive public sector use should therefore specify open-weight model availability as an eligibility condition: a provider supplying only proprietary closed-weight API access is creating an architectural dependency that no portability clause can resolve after the fact.

The principle is constant across all layers : the DC-EDIC defines the floor and providers compete above it. European public sector procurement enforces the floor as an eligibility condition, not as a scoring criterion. This converts the DC-EDIC's technical work into a market signal: the providers that meet the floor can access one of the largest technology markets in the world. The providers that do not, can not.

The precedents are available. GSM was a European standard that reshaped global telecommunications not by building a European phone manufacturer but by mandating a protocol that all operators had to support to access the European market. SEPA created a sovereign European payment rail not by building a European bank but by mandating the clearing protocol through which all eurozone banks must operate. The DC-EDIC has the institutional mandate and the technical expertise to do the same for cloud portability, identity federation, and open-weight AI. What it requires is the political commitment of its founding member states to translate its technical definitions into procurement eligibility conditions.

4.4 - The procurement lever: create the demand signal European providers cannot generate alone

European public sector technology procurement is, in aggregate, one of the largest technology markets in the world. Its collective scale is not reflected in its collective behaviour, because procurement decisions are made in thousands of independent processes under identical structural incentives, producing the aggregate outcome described in section 1.

Two mechanisms would change that dynamic, each with a documented operational precedent.

The first is a joint procurement framework for sovereign cloud and software services, modelled on the European Defence Agency's joint procurement architecture for defence capabilities. The EDA coordinates member state demand for common defence requirements, aggregating purchasing power that no individual member state could deploy alone and creating the commercial viability signal that European defence industry requires to invest at scale. The same logic applies to cloud infrastructure, identity management, and endpoint security: the individual procurement volumes of even large member states are insufficient to anchor the investment cycles European providers need to close the capability gaps identified in section 2. A joint procurement framework coordinated at

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

EU level, with standardised sovereignty criteria derived from the finalised EUCS, would aggregate that demand without requiring member states to surrender procurement autonomy.

The second is a pre-qualification catalogue for sovereign digital services, the procurement-layer equivalent of FedRAMP. Its function is to absorb the per-organisation compliance verification cost that currently acts as a transaction cost on every attempt to procure a European alternative. A public sector procurement officer who can draw from a pre-qualified catalogue of EUCS-certified European providers (cloud infrastructure, IAM, endpoint security, collaboration tools) does not need to commission an independent security assessment to justify the procurement decision. The reduction in administrative friction is itself a sovereignty instrument: it levels the procurement playing field between established American platforms, which benefit from years of accumulated procurement familiarity, and European alternatives that are technically competitive but administratively unfamiliar.

Two instruments would reinforce the procurement framework without requiring additional legislative vehicles.

The first is mandatory exit cost disclosure. European public organisations discover the real cost of leaving an American platform when they attempt to leave it. A requirement integrated as a condition of EUCS pre-qualification, obliging providers to communicate annually to their public sector clients the estimated migration cost, the available export format for all data categories, and the architectural dependencies created by the contract, would make lock-in visible before a contract is renewed rather than after it is contested. The Data Act's switching assistance obligations set a floor for data portability. This requirement raises it by converting an unknown into a documented, annually updated figure that procurement officers can include in their renewal assessments.

The second is the training of public procurement officers. The vendor evaluation framework proposed in Annex C has operational value only if the people applying it have been trained to use it. The initial and continuing training of procurement officers in European administrations does not currently cover digital sovereignty criteria in any systematic way. Integrating a mandatory module on sovereignty assessment into the training curricula of the institutions that prepare senior civil servants and procurement specialists, at national level through bodies such as the INSP in France and the Bundesakademie in Germany, and at European level through the European Institute of Public Administration, creates multiplier agents in every contracting authority without requiring a central enforcement body.

4.5 - The role of Member States: build the consensus, do not replicate the effort

The institutional work already done at member state level is genuine and significant. ANSSI's SecNumCloud framework is the most technically rigorous cloud security certification in Europe. Germany's Sovereign Tech Fund provides public investment in open-source infrastructure that the market will not fund alone. The Franco-German digital sovereignty commitments of November 2025 represent the most explicit bilateral political signal on this agenda in a decade. DINUM's Suite

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Numérique, despite the adoption challenges documented in section 2.4, has produced operational open-source tools that have been deployed at speed by institutions facing active dependency activation.

Each of these initiatives is a national response to a structural problem that is European in scale. The gap between what they have produced and what the dependency map of section 2 requires is a function of the coordination layer above them that does not yet exist. The collective action problem described in section 1.3 produces national champions that cannot reach European scale, certification frameworks that are not mutually recognised across all member states, and procurement signals that are too fragmented to anchor the investment cycles European providers need.

A further instrument addresses foundational infrastructure gaps that neither procurement frameworks nor interoperability standards can reach: direct public investment in open-source infrastructure that the market will not self-fund. Germany's Sovereign Tech Fund, which finances the maintainers of critical open-source components embedded in European digital infrastructure, and the European Commission's Next Generation Internet programme under Horizon Europe, which funds open protocol development, are both operational models for this logic. Both operate on the same logic that certain infrastructure layers function as public goods: no commercial actor has the incentive to build them unilaterally, their absence creates dependencies that accumulate invisibly until they are activated, and their development requires public capitalisation rather than market incentive. The terminal attestation layer documented in section 2.5 illustrates the pattern precisely. The dependency is structural, the European technical capacity to address it exists, and the missing variable is the public investment signal that makes a consortium viable and its output durable. A systematic programme extending the Sovereign Tech Fund model to dependency gaps identified through assessments of the kind this report provides would convert that signal into a repeatable instrument, applicable wherever a foundational open-source alternative exists in nascent form but lacks the capitalisation to reach operational maturity.

The most valuable action Member States can take is to use their existing bilateral and multilateral relationships (including, but not limited to the Franco-German axis in particular, given its documented track record in initiating European-scale digital policy) to build the political consensus for the four decisions described in this section: the combination of sectoral sovereignty mandates and the CADA legislative process, extending the Interoperable Europe Board's mandate to cover collaboration and identity federation standards, establishing a joint procurement framework with pre-qualified sovereign providers, and directing the DC-EDIC to define binding workload portability floors by layer. All four are consolidated with their institutional owners and progress signals in Annex G.

4.6 - Transmitting the signal: governance and communication

The levers described in sections 4.1 to 4.5 operate at the level of institutions that already understand the dependency problem. A harder question that needs answering is how the assessment reaches the decision-makers who have not yet connected it to a decision within their authority.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The gap between technical awareness and governance action is not primarily an information problem. Cybersecurity agencies, parliamentary committees, and expert assessments have documented the dependency landscape for years. The failure is in the transmission chain between the organisations producing this analysis and the leaders holding authority to act on it.

Two mechanisms have reliably produced governance change at scale in analogous domains in Europe.

The first mechanism is financial liability calibrated to organisational scale. The GDPR produced Data Protection Officers in every organisation within scope not because it mandated good data practice in general terms, but because its fines, expressed as a percentage of global annual turnover, made non-compliance a board-level financial risk rather than a technical department problem. NIS2 replicates this architecture for cybersecurity: Article 21 requires documented risk management measures including supply chain dependencies, and the supervisory fines available under the directive are proportional to turnover in ways that make unmanaged exposure a material item for executive committees. ANSSI Director General Vincent Strubel made this point explicitly before a Senate inquiry: it is the proportional fine, not the theoretical personal liability of directors, that reliably brings cybersecurity topics to the attention of governing bodies. An organisation that has not documented its critical digital dependencies under NIS2 Article 21 already carries a potential compliance gap whose financial consequence is calculable as a fraction of its annual revenue. Framing the dependency audit as a NIS2 compliance obligation rather than a sovereignty aspiration connects it to a mechanism that executive committees already have processes for managing.

The second mechanism is communication routed through channels calibrated to each decision-making audience. The technical community producing dependency assessments communicates through technical channels: agency publications, specialist conferences, expert press. These channels reach technical staff who already share the diagnosis but do not reach the directors general who control budget authority, the elected officials who set legislative agendas, or the board members who govern private sector organisations.

Each of these audiences has its own channels and its own vocabulary of risk. Directors general of public administrations respond to findings from national courts of accounts, which have the mandate and the credibility to audit public sector digital dependency exposure and issue recommendations with formal follow-up requirements. The Cour des Comptes in France and the Bundesrechnungshof in Germany have already produced reports on adjacent governance failures. An audit specifically targeting unmanaged digital dependency exposure would reach ministerial cabinets in a register that no expert report can match. Elected officials respond to constituent concerns and to the framing of risks in terms of political consequence: the ICC case documented in the introduction to this report is more legible to a parliamentarian as a story about European citizens being excluded from their own banking system than as a jurisdictional dependency analysis. Private sector board members respond to audit committee findings and to peer organisation decisions. The accounting dimension of unmanaged operational risk, described in section 5.3, is the language through which this analysis reaches governance structures outside the public sector.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

What this requires from the institutions addressed in sections 4.1 to 4.5 is not a communication campaign in the conventional sense. It is the deliberate routing of the same analysis through channels calibrated to each decision-making audience, consistently, over a period long enough to shift the reference frame within which individual governance decisions are made. The sectoral professional federations present in every regulated sector, banking, healthcare, energy, local government, are the natural intermediaries for this routing: they have the convening authority to make digital dependency assessment a standing governance topic in formats that reach their members' leadership without requiring those leaders to read technical assessments they will not read.

4.7 - Taking the initiative: from defensive posture to structural leverage

The levers described in sections 4.1 through 4.6 are predominantly defensive. They reduce exposure, raise switching costs for incumbents, and create conditions under which European alternatives can compete. Their logic is reactive by construction: each addresses a bias, an imbalance, a dependency that has already formed. The dependency map of section 2 was not created by inattention alone. It was created because the structural incentives of the market, the lobbying capacity of incumbent platforms, and the collective action failures of European procurement consistently favoured the status quo. Reducing existing dependencies without changing those structural incentives produces a report but not a trajectory.

Six instruments are available to European decision-makers that operate on the causal level rather than the symptomatic one.

Lever 1: European public data as a strategic asset

European public administrations collectively hold datasets that have no equivalent elsewhere: multilingual health records covering populations governed by a single regulatory framework, judicial data across multiple legal traditions, administrative records, and high-resolution geospatial data. These datasets are currently either closed or accessible without sovereignty conditions. They are also among the most valuable training inputs for AI models serving European-language, European-legal, and European-administrative use cases. Those are precisely the verticals where European providers like Mistral can build a durable competitive advantage over American generalist models.

Vehicle: a Commission implementing act under the Data Governance Act (Article 3, conditions for re-use of protected public sector data) combined with a Council recommendation on AI training data access conditions. The Data Governance Act already provides the legal basis for member states to impose conditions on the re-use of public sector data for purposes of general interest; an implementing act specifying sovereignty of infrastructure as a mandatory condition for AI training use would require no new legislative vehicle. ENISA and the AI Office are the natural bodies to define the technical annex specifying what "sovereignty of infrastructure" means in operational terms, drawing directly on the SecNumCloud, C5, and ENS frameworks.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Current blocker: the default position of most European administrations is that public data held by government bodies is either closed (not accessible at all) or open (accessible without conditions). The intermediate category (conditionally accessible for AI training under sovereignty constraints) has no established procurement or licensing infrastructure. Building that infrastructure requires a political decision to treat public data as a strategic asset rather than a governance object. That decision has not been taken at European scale.

Progress signals: a Commission communication explicitly framing public sector data as an input to European AI competitiveness, with conditionality tied to infrastructure sovereignty. At least one member state (France is the most likely candidate given the Mistral relationship and the existing health data governance framework) establishing a conditional AI training data access programme with documented sovereignty requirements. An ENISA technical standard specifying the infrastructure conditions under which public sector data can be made available for AI training.

Realistic horizon: 2027 for a Commission implementing act, contingent on political commitment from the current Commission college. National programmes could move faster: 2026 is achievable for a French pilot in the health data domain, where the governance architecture already partially exists.

Lever 2: Reciprocity in public procurement

The International Procurement Instrument (IPI), which entered into force in 2022, allows the European Commission to restrict access to European public procurement markets for suppliers from countries that do not offer reciprocal access to European companies. The American federal technology procurement market is substantially closed to European suppliers in categories directly relevant to this report: cloud infrastructure, identity management, and cybersecurity software for sensitive government use. The IPI has not been activated against the United States in any technology category as of the publication date of this report.

Vehicle: the International Procurement Instrument (IPI, Regulation EU 2022/1031), which entered into force on 30 August 2022. The IPI allows the Commission to launch an investigation into market access restrictions, issue a report, and if the finding is confirmed, restrict third-country suppliers' access to EU public procurement above specified contract value thresholds. No new legislation is required. The Commission can open an IPI investigation on its own initiative or following a member state or industry request. The investigation phase takes twelve months and a measure, once adopted, can be suspended if the third country opens negotiations on market access improvement.

Current blocker: the Commission has opened IPI investigations in several sectors (Chinese medical devices, Chinese electric vehicles) but has not applied the instrument to digital technology procurement, where the market access asymmetry between the EU and the United States is arguably more measurable and more documented than in any physical goods category. The political cost of

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

activating the IPI against the United States is higher than against China and is the main blocker in this case.

Progress signals: a Commission market access investigation into U.S. federal technology procurement barriers, formally launched under IPI Article 5. A member state formal request triggering that investigation. A Commission communication explicitly linking IPI activation readiness to progress on bilateral digital trade negotiations with the United States, creating a credible threat without requiring immediate activation.

Realistic horizon: an IPI investigation could be launched within the current Commission mandate (before 2029) if political will exists. The credible threat of activation is available immediately and costs nothing to signal. Full activation and a resulting procurement restriction measure: 2027 at the earliest given the investigation timeline.

Lever 3: Exporting the standard rather than defending it

The “Brussels effect”[147] produced durable results on data protection: third countries adopted GDPR-equivalent frameworks because access to the European market required compliance, and because a single framework was more efficient than fragmented national ones. The same dynamic is available to European digital sovereignty instruments if they are designed with export in mind from the outset. Japan, South Korea, Canada, and a significant share of the Global South share the same fundamental concern documented in this report: operational, jurisdictional, economic, and normative dependency on a small number of American technology platforms. They lack a coherent alternative framework.

Vehicle: the EU's existing digital diplomacy infrastructure, specifically the EU Cyber Diplomacy Toolbox, the Global Gateway digital connectivity component, and the bilateral digital partnerships the Commission has established with Japan (2022), South Korea (2023), and Canada (2023). These partnerships already include commitments on regulatory cooperation and standards alignment. Extending them to include technical assistance for the adoption of EUCS-equivalent certification frameworks and DC-EDIC portability standards would require a political decision at the partnership committee level but no new legislation. The ASEAN Digital Integration Framework and the African Union's data governance agenda are the most promising near-term targets for a standard-export strategy given the scale of the dependency problem in those regions and the absence of an established alternative framework.

Current blocker: European digital diplomacy is currently oriented toward promoting the GDPR as a data protection standard and toward connectivity investment through Global Gateway. It does not yet systematically promote European cloud security and sovereignty standards as exportable frameworks. The institutional capacity for standard-export diplomacy (technical attachés in partner country delegations, training programmes for third-country regulators, model legislative text) does not yet exist at the scale that would make the strategy effective.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Progress signals: explicit inclusion of EUCS-equivalent certification adoption in the technical annexes of EU digital partnership agreements with at least three partner countries. A Commission digital diplomacy programme specifically funding third-country regulatory capacity building around European cloud sovereignty standards. An ENISA international cooperation mandate extended to cover technical assistance to non-EU regulatory bodies.

Realistic horizon: 2026 for the inclusion of standard-export language in renewed digital partnership agreements (the Japan and South Korea partnerships are both up for review within this horizon). Meaningful third-country adoption: 2028 at the earliest for the most receptive partners.

Lever 4: Shared sovereign compute infrastructure

The AI investment asymmetry documented in section 2.7 (roughly 30 to 1 in favour of the United States in 2024 private investment) cannot be closed through organic market development alone. European AI capability is bounded at the infrastructure layer by access to GPU compute, which is concentrated in American-designed hardware and American-operated cloud capacity. Individual member state programmes (France's Plan IA, Germany's AI compute initiatives) produce national capacity that falls short of the threshold required for frontier model training and for the managed inference services that public sector organisations need.

Vehicle: the DC-EDIC, whose statutory mandate explicitly covers AI infrastructure as a domain of cross-border open-source digital infrastructure development. The DC-EDIC's founding member states (France, Germany, the Netherlands, Italy) collectively represent sufficient political and financial weight to capitalise a shared compute facility at meaningful scale. The legal structure already exists in European law, in the forms of an ERIC (European Research Infrastructure Consortium) or a treaty-based intergovernmental organisation modelled on CERN. The EuroHPC Joint Undertaking, which operates seven petascale supercomputers across Europe under a similar multi-member governance structure, provides the closest operational precedent: it was created in 2018, reached operational capacity in 2021, and demonstrated that collective European investment in shared scientific infrastructure can produce world-class facilities within a single parliamentary term.

Current blocker: EuroHPC's mandate is scientific research, not commercial AI inference or public sector deployment. Extending it or creating a parallel structure to cover AI compute accessible to administrations and European AI providers requires a political decision to treat AI infrastructure as a public good rather than a market outcome. That decision has not been taken yet. Individual member state programmes (France's Plan IA 2030 funding compute investment, Germany's AI compute strategy) remain nationally siloed and fall short of the threshold required for frontier model training.

Progress signals: a DC-EDIC Governing Board resolution mandating a feasibility study for a shared European sovereign AI compute facility, with a defined minimum compute target and an access condition framework excluding non-EU-owned operators. A formal Commission proposal to extend

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

the EuroHPC mandate to include AI inference capacity accessible under sovereignty conditions. A joint Franco-German commitment to co-finance the initial capitalisation of such a facility, creating the core around which other member states can aggregate.

Realistic horizon: feasibility study and political commitment: 2026. First operational capacity: 2028-2029, consistent with the pace of the EuroHPC deployment cycle.

Lever 5: Addressing the lobbying asymmetry

The industry lobbying capacity documented in section 1.1 (€151 million annually, more lobbyists in Brussels than MEPs in the Parliament) is structural. It reflects the margin economics of platform businesses: a €1 spent on lobbying that preserves a €100 revenue stream is a rational investment at any scale. The European ecosystem of sovereign digital alternatives does not operate at margins that support equivalent lobbying investment. The result is a systematic imbalance in the information environment within which regulatory decisions are made: Commission officials, MEPs, and member state civil servants are exposed to far more sophisticated, better-resourced, and more consistently sustained advocacy from incumbent platforms than from the providers this report identifies as alternatives.

Vehicle: a European Commission grant programme under the Digital Europe Programme (DEP), which already funds digital capacity building across member states and includes civil society and industry association eligibility. A dedicated DEP call for proposals targeting advocacy capacity for European digital sovereignty actors, with eligibility conditions tied to the ownership test applied throughout this report, would not require new legislation and could be operational within a standard grant cycle. The Open Internet Act in the United States provides a partial precedent for public funding of civil society digital rights advocacy, though its scope and structure differ. The European Parliament's own budget line for civil society digital rights organisations is a closer model.

Current blocker: the framing of this instrument as "lobbying funding" creates political sensitivity that the framing of "regulatory capacity building" does not. The substance is identical but the political palatability differs. A Commission call framed around "independent technical expertise in digital sovereignty standards processes" (with deliverables tied to consultation submissions, technical working group participation, and regulatory impact assessments) addresses the same gap without the political cost of appearing to fund lobbying.

Progress signals: a DEP call for proposals explicitly targeting independent technical expertise in digital sovereignty standards processes, with a minimum budget of €20 million over three years. At least three organisations representing European sovereign digital providers receiving funding under this programme and demonstrating sustained participation in EUCS, DC-EDIC, and Interoperable Europe Board processes. A Commission commitment to publish an annual report on the balance of representation in its digital standards consultation processes.

Realistic horizon: a DEP call could be launched within the current multiannual financial framework without requiring a budget revision. 2026 is achievable for a first call, grantees operational by 2027.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Lever 6: Antitrust enforcement as a deterrent instrument

The antitrust tools available to the European Commission and national competition authorities are among the most powerful available to any regulatory body in the world. The Digital Markets Act designates gatekeepers and imposes obligations whose violation carries fines of up to ten percent of global annual turnover, with structural remedies available for repeated infringements. These instruments already exist and their deterrent effect depends entirely on the speed and predictability of their application.

Vehicle: the Digital Markets Act, specifically Articles 26 and 27 (non-compliance investigations and fines), Article 24 (interim measures in urgent cases), and Article 29 (structural remedies for systematic infringement). The DMA enforcement architecture is fully operational: the Commission designated six gatekeepers in September 2023 and has opened non-compliance proceedings against Apple, Alphabet, Meta, and Microsoft. What is missing is systematic use of interim measures (available where there is urgency due to the risk of serious and irreparable harm to contestability or fairness in core platform services) in cases directly relevant to the dependencies documented in this report.

Current blocker: the Commission has used interim measures once under the DMA as of the publication date of this report (against TikTok in a case unrelated to the dependency layers documented here). The political cost of interim measures against American companies in the current geopolitical context, documented in the introduction through the White House memorandum of February 2025 and the threatened Section 301 investigation, creates a deterrent effect on enforcement aggressiveness that is not legally justified but is politically real. Enforcement speed is also structurally constrained by the Commission's investigative capacity: the DMA enforcement team is substantially smaller than the lobbying apparatus it is designed to regulate.

Progress signals: use of DMA Article 24 interim measures in at least one case directly relevant to the interoperability or switching cost obligations most relevant to this report (messaging interoperability, cloud switching assistance, identity federation). A Commission commitment to publish enforcement timelines for all open DMA proceedings, with a stated objective of completing non-compliance investigations within eighteen months of opening. A Council conclusion explicitly linking DMA enforcement speed to European digital sovereignty objectives, providing political cover for aggressive enforcement posture.

Realistic horizon: interim measures in a relevant case: possible within the current Commission mandate if political will is applied. Systematic enforcement acceleration depends on the Commission staffing the DMA enforcement team at a level commensurate with its mandate, a condition that has not been met. In April 2025, outgoing DG COMP Director-General Olivier Guersent stated publicly that the department was more than 200 staff short of being able to properly enforce the DMA alongside its other responsibilities, and was being forced to deplete other departments to balance its priorities.[148]

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Section 5 - What a public organisation can do

Sections 2 and 3 established what is exposed and under what conditions. Section 4 identified the levers that operate above the organisational level. This section operates at a different altitude: what a single organisation can decide, resource, and execute without waiting for European coordination, regulatory resolution, or political consensus.

The boundary between what is within organisational reach and what is not is drawn explicitly throughout. Some dependencies documented in section 2 can be addressed within a procurement cycle. Others require coordinated action that no single organisation can drive alone. Conflating the two produces either paralysis, because the hardest problems seem unsolvable, or false confidence, because the solvable ones seem sufficient. The prioritisation logic that follows is designed to prevent both.

One objection applies specifically to the organisational level and will get a direct answer here: the claim that migration is simply too expensive. For the organisational migrations documented in this section, the financial case is consistently positive. The Schleswig-Holstein benchmark (section 5.1) and the Échirolles case document returns on investment within one to three years at all scales of public administration. The argument that migration is too expensive does not apply to procurement decisions that have a documented payback period shorter than the contract horizon against which they are evaluated. It would apply if this report were recommending a centrally planned, simultaneously executed European migration programme at EU scale, which it is not. The operational facet of this report aims to highlight the conditions under which individual organisations can act, and to give each organisation the tools to construct its own financial case. That financial case, at organisational scale, is systematically positive. The question is therefore not whether migration is affordable but whether the capital for the one-time cost is available within the organisation's planning cycle, which is the question sections 5.2 and 5.3 address directly.

The full alternatives table (Annex D) and decision ownership matrix (Annex G) are the primary tools for implementation. Operational readers are encouraged to consult them directly.

5.1 - The prioritisation matrix

Not all dependencies warrant the same response, and not all migrations are equally accessible. Treating every exposure as an emergency produces paralysis, and treating none as urgent produces the outcome documented in section 3. The matrix that follows gives every organisation a framework for arbitrating between the two.

The framework operates on two axes. The vertical axis measures dependency level, rated CRITICAL, SERIOUS, or MANAGEABLE as defined in the methodological note: how severely would operational continuity be affected by failure or denial of service at this layer? The horizontal

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

axis measures migration feasibility: is a credible European alternative available at production maturity today, and can migration be executed within a normal budget and planning cycle without exceptional political commitment?

The intersection of these two axes produces four distinct situations, each of which calls for a different response.

Quadrant 1 - Migrate as a priority

Critical dependency. Accessible migration.

This quadrant describes an organisation whose most exposed layer has a viable European alternative available today. The dependency is real and the switching cost is manageable. Deferral is not a neutral choice: it deepens lock-in with every contract renewal and every new integration built on top of the incumbent platform.

The clearest example at this level is an organisation whose core workloads are standard office productivity (document creation, email, calendar, file storage, video conferencing) running on Microsoft 365, with no deep integration of Azure-specific managed services into business-critical applications. For this profile, European alternatives exist at production maturity. The migration is organisationally demanding but technically straightforward, and its financial case is documented.

The Schleswig-Holstein migration, documented in full in section 6.2, is the closest available benchmark for a mid-sized public administration with standard office productivity workloads: €9 million one-time cost against annual savings exceeding €15 million from 2026[149], a payback period of under one year.

The analytics migration documented in section 2.6 (i.e. replacing Google Analytics with a self-hosted Matomo instance) is the most bounded available illustration of this quadrant's logic: the dependency is a documented GDPR violation, the European alternative is production-mature and free, and the migration is technically trivial. It requires no budget approval, no political mandate, and no external coordination.

Quadrant 2 - Plan with dedicated resources

Critical dependency. Structurally difficult migration.

This quadrant describes an organisation where the dependency is severe and the migration is not accessible within a normal procurement cycle. The combination of deep technical integration, operational continuity requirements, and the absence of drop-in alternatives means that migration requires a multi-year programme with dedicated budget, executive sponsorship, and political backing. Deferral here is not neutral either, but the appropriate response is structured planning rather than immediate technical action.

The most documented European case at this level is France's Health Data Hub. Created in 2019 to centralise secure researcher access to French health data including the *Système National des*

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Données de Santé, the platform has been hosted on Microsoft Azure since inception, a choice that generated sustained legal and regulatory challenge from the CNIL, the *Conseil d'État*, and successive parliamentary inquiries. The CLOUD Act exposure (the fact that Microsoft, as a U.S.-incorporated company, is subject to American government data demands regardless of where data is physically stored) was identified as structurally incompatible with the platform's function as a repository for the health data of 67 million French citizens.

In February 2026, the government launched a procurement process under the UGAP Nuage Public framework conditioning eligibility on sovereignty certification equivalent to SecNumCloud[150]. Microsoft is not SecNumCloud-qualified. The government confirmed publicly that American hyperscalers are structurally excluded from this process.[151] The precise certification criteria in the procurement documentation were not publicly disclosed at the time of writing, and at least one market participant contested the government's characterisation of the eligibility conditions.[152] The contractual award was expected by end of March 2026 with full migration targeted by end of year.

The juxtaposition is analytically significant: the Conseil d'État validated a transitional arrangement on the same day the government was conducting a procurement to replace it under criteria that exclude the current provider. The technical migration is achievable but the governance cost of seven years of deferred decision, marked by successive reversals, contradictory arbitrations, and legal proceedings, is not recoverable.

For any organisation in this quadrant (a regional hospital with clinical systems integrated into Azure infrastructure, a ministry whose business applications authenticate exclusively through Entra ID, a national agency whose data pipelines run on AWS-specific managed services) the appropriate response is a structured programme with a named executive owner, a realistic multi-year horizon, and a formal risk register that documents the exposure under NIS2 obligations until migration is complete.

Quadrant 3 - Capture at renewal

Lower criticality. Accessible migration.

This quadrant describes a dependency that is real but not acute, and for which migration is feasible without exceptional resources. The appropriate response is not immediate action but deliberate preparation: sovereignty criteria built into the next procurement cycle, so that the dependency is not renewed on identical terms at the next contract expiry.

A university operating student communication and collaboration tools on Google Workspace is a representative profile. The exposure is genuine (CLOUD Act jurisdiction, data residency, normative lock-in) but the operational consequences of a service disruption are not comparable to those of an IAM failure or a payment processing outage. The European alternatives are mature. The migration window is the contract renewal, and the preparation required is a sovereignty assessment conducted before that renewal, not after.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The procurement lever identified in section 4.3 is most directly actionable for organisations in this quadrant: building sovereignty criteria into the renewal process costs nothing if done at the right moment in the procurement cycle and and the full price of another contract term if done too late.

Quadrant 4 - Document, accept residual risk and monitor for developing solutions[2]

Lower criticality. Structurally difficult migration.

This quadrant describes a dependency for which no credible European alternative currently exists at the required level of operational maturity, and whose criticality does not justify absorbing the cost and disruption of a migration to a partial substitute. The appropriate response here is governance: formal documentation of the exposure, monitoring of the European alternatives landscape, and participation in the policy processes that can change the conditions under which the dependency persists.

A national statistics agency whose analytical pipelines depend on AWS-managed services (Redshift, Athena, SageMaker) with no European equivalent of comparable catalogue depth and no internal capacity to rebuild the architecture around provider-agnostic components is a representative profile. The dependency is real but the migration is not feasible within any planning horizon the organisation controls. The honest response is to say so, document it formally, and monitor.

The NIS2 Directive provides the governance vehicle: Article 21's risk management obligations require organisations to identify, assess, and formally manage their operational dependencies. A dependency that cannot be resolved within the organisation's decision horizon is not exempt from NIS2 obligations. Such dependencies represent a risk to be documented, reported, and escalated to the level at which it can be addressed. That is the level described in section 4.

Applying the matrix

The four quadrants are not permanent classifications. A dependency that sits in Quadrant 4 today may move to Quadrant 2 as European alternatives mature, or to Quadrant 1 if the geopolitical context elevates its criticality. The matrix is a living governance instrument, not a one-time exercise. Its value is in forcing an explicit answer to two questions that most organisations have not systematically asked: how severe is this dependency if activated, and how accessible is the exit?

Migration horizons by organisational scale, including the enabling preconditions for each profile, are in section 6.5.

Migration sequencing: the logic behind the order

A sequencing logic emerges from the documented cases. Each step reduces the retraining cost and operational risk of the next. Disrupting the sequence creates the conditions for the failures that have ended migration programmes before completion.

2 The abbreviated Executive Summary title for this quadrant is *Reduce exposure now* to emphasize actions to be taken

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Analytics, CDN, and DNS migrations are invisible to end users, technically trivial, and executable within normal operational budgets in days to weeks. Web analytics migration resolves a documented GDPR violation. CDN migration requires a DNS record change. Neither demands user retraining, architectural rethinking, or executive sponsorship. They establish whether the organisation can move at all.

Internal messaging migration involves end-user change at low operational stakes: no documents are lost, no workflows are interrupted, and the tool operates in parallel with, for example, Microsoft Teams for external contacts during the transition. The change management competence it builds is directly transferable to the productivity suite migration that follows.

IAM preparation must begin in parallel from programme initiation. If applicable, Keycloak must be deployed alongside Entra ID from the outset, expanding its scope progressively across internal applications. It requires months to reach stable production coverage and cannot be compressed into a crisis timeline. An organisation that begins Keycloak deployment on the day it decides to migrate its productivity suite has already lost the lead time its most critical dependency requires. IAM is not a late-stage migration but a parallel workstream that must start early.

Office document creation, email, calendar, and file storage are the highest-visibility user-facing change and the most significant change management challenge in the stack. The Schleswig-Holstein and Gendarmerie cases applied the same sequencing: open-source applications deployed in parallel under the incumbent operating system, document format standards mandated before forced removal, the hardware replacement cycle used to absorb the transition progressively. Users who have already been working in LibreOffice under Windows for six months absorb the operating system change at a fraction of the cost.

Cloud IaaS migration does not require end-user change and can proceed on a separate track, moving at the pace of the architecture assessment rather than the change management programme.

HarfangLab and Tehtris can be deployed alongside an existing American EDR on the same endpoints without a detection gap. This is the only migration in the standard stack for which parallel operation is normal deployment practice rather than a transitional compromise.

The operating system migration depends on stable IAM coverage, familiarity with open-source tools already established through prior migrations, and a completed application compatibility assessment. The organisations that have stalled at OS migration have typically attempted it before those conditions were met.

The financial dimension

The financial case for beginning is straightforward: migration costs are bounded and documented, while the cost of deferral accumulates with every contract renewal and every new integration added to an incumbent platform. An administration that extends its Microsoft 365 agreement by three years, expands its Azure footprint, or adds business applications authenticating through Entra ID does not avoid the eventual migration. It does, however, raise its cost.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The Schleswig-Holstein benchmark quantifies the asymmetry at the scale of a mid-sized administration. One-time migration cost: approximately €300 per workstation. Annual savings from year one: more than €500 per workstation. An organisation that defers five years loses the equivalent of the migration budget in licence expenditure that would already have been redirected to European providers. The preparation costs a fraction of the migration. The migration conducted under pressure, without prior preparation, costs a multiple of the migration planned in advance.

The figures below are indicative orders of magnitude derived from the Schleswig-Holstein benchmark for the two largest scales, and from the Échirolles benchmark for the smallest scale. They cover office productivity suite, email, and file storage migration. IAM migration requires a dedicated programme budget not included here. Operating system migration is absorbed progressively through the hardware replacement cycle at minimal marginal cost once the application layer is stable.

Organisational profile	One-time migration cost	Annual savings from year 1	Indicative payback
Small municipal administration (up to 500 agents)	€50,000 - 150,000 (staff time and external support)	€80,000 - 150,000	12 - 36 months
Regional administration (up to 5,000 agents)	€1.5M - 3M	€2M - 4M	8 - 15 months
Ministry or large national agency (50,000+ agents)	€12M - 25M	€20M - 35M	7 - 12 months

Annual savings represent licence costs redirected from American platforms to European providers and local support contracts, not a net reduction in total IT expenditure. The financial case is positive at all three scales. The constraint at smaller scales is capital availability for the one-time investment, not the return on it.

At the smallest profile, the one-time cost is within the discretionary budget of a single IT procurement cycle for most French and German municipalities.

The most directly usable financial benchmark for the small administration profile is the municipality of Échirolles (Isère, France, c. 37,000 inhabitants), which adopted a digital sovereignty mandate by unanimous council vote in 2021 and has progressively migrated its infrastructure to open-source platforms since that date. The migration was structured around a voluntary adoption model, beginning with the Head of Digital Strategy himself, and absorbed through the hardware replacement cycle rather than funded as a capital programme. On a total IT budget of approximately €1 million, the municipality documents annual licence savings of approximately €350,000 (self-reported figure, not independently audited), representing cumulative savings of €2 million over the 2021-2026 mandate[153] [154] [155]. The IT budget has remained stable or declined over the same period while the functional scope of digital services has doubled[156]. Migration to Linux (Zorin OS) began in 2024 on a voluntary basis, targeting 10% of the 1,500-workstation fleet in the first year[157]. Nicolas Vivant, the municipality's Head of Digital Strategy, has noted that the voluntary adoption

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

phase is itself a sequencing instrument: it identifies the population of early adopters who then serve as internal peer references for the broader rollout. The absence of a dedicated change management budget is not a generalised recommendation. It reflects a specific institutional choice to use social proof rather than formal training as the primary adoption driver, a model that transfers most readily to administrations with visible internal champions and sustained political commitment at the mayoral or directorial level[158].

The one-time cost mentioned for Échirolles represents staff time and external support rather than capital expenditure, though it must be stated that those costs are drawn from municipal communications and local press, and have not been subject to independent audit. The Schleswig-Holstein benchmark (section 6.2) remains the only fully published and externally-audited figure with an explicit one-time cost and annual saving, figures for the two other profiles should be verified against the organisation's own licence structure before use in a budget submission.

At the largest, the payback period is shorter than the typical three-year IT contract horizon against which the investment would be evaluated. Framing the migration as a capital expenditure requiring exceptional budget authority applies the wrong financial model: it is a cost substitution with a documented payback under two years.

The organisations that fared best when dependencies were activated were not those with the largest IT budgets. They were those that had already asked how severe each dependency would be if activated, how accessible the exit was, and had taken the specific actions that the answers to these questions required.

5.2 - Within six months: actions requiring no additional budget

Map the stack. Produce a complete inventory of every digital service in operation: provider, contractual relationship, data categories processed, hosting location. Apply the four dependency dimensions from the methodological note to each service and flag any that creates exposure across two or more simultaneously. Most organisations will find between five and fifteen critical dependencies. The inventory is not a one-time exercise. The ownership provenance of any provider must be verified at each renewal cycle, for the reasons documented in section 1.4.

Read the contracts. For every critical dependency, four clauses warrant explicit attention: CLOUD Act exposure (does the provider have a U.S.-incorporated parent?), termination conditions and notice period, data portability terms and format on exit, and renewal date. The renewal date is the action window. An organisation that does not know when its Microsoft 365 contract renews cannot act at the right moment.

Identify and brief. From the dependency map, identify the three services whose simultaneous unavailability would most severely degrade core functions. For most European public organisations these will be the identity provider, the collaboration suite, and the primary cloud environment. Name them explicitly, with the American corporate entity whose decision could interrupt each, and

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

the estimated time to operational failure without prior preparation. Translate this into a governance briefing addressed to the Director General or equivalent. The gap between what technical staff know about dependency exposure and what executive leadership knows is itself a governance risk. Under NIS2 Article 20, it is also a legal one.

First actions, executable in weeks

The actions below require no budget approval, no formal programme, and no external coordination. Each can be initiated by a single IT manager or a small team acting within existing operational authority. Their primary function is not strategic transformation. Each one tests whether the organisation can move at all, builds a bounded unit of migration competence, and creates a documented result that informs the larger decisions that follow.

- *Replace Google Analytics with a self-hosted Matomo instance.* The CNIL ruled in 2022 that Google Analytics transmissions constitute a GDPR violation. The legal position is unambiguous and documented in section 2.6. Matomo is production-mature, self-hostable within the organisation's own infrastructure, GDPR-compliant by architecture, and available at zero licence cost. Migration for a standard institutional website is achievable within days by a single developer. It is the most bounded available test of whether the organisation can substitute an American platform dependency with a European alternative: the technical complexity is minimal, the governance requirement is absent, and the outcome is a documented GDPR remediation that costs nothing and takes a week.

- *Deploy an internal artifact proxy.* Any organisation developing or maintaining software pulls build dependencies from npm, PyPI, or Docker Hub at compile time. An internal artifact cache intercepts those requests, stores local copies of approved packages, and allows builds to complete without live access to American-controlled registries. Mature open-source tools for this purpose exist and are documented in section 2.8. Deployment is achievable within weeks on existing internal infrastructure. The result addresses both the sovereignty exposure and the supply chain integrity risk that direct registry dependency creates. It does not require a migration programme or exceptional budget.

- *Audit Entra ID integration depth across the application portfolio.* An organisation that does not know which of its business applications authenticate exclusively through Microsoft Entra ID cannot triage its IAM dependency. This audit requires no tooling beyond access to the application registry: for each application, one question must be answered and documented. Does it authenticate through Entra ID, and if so, does it have any alternative authentication path? The output is a list of applications that would lose access simultaneously if Entra ID were suspended, ordered by operational criticality. This list is the prerequisite for any IAM migration planning. The audit is executable by an IT manager in days and produces the single most operationally useful document an organisation can have before beginning a migration programme.

- *Migrate CDN and DNS to a European provider for at least one public-facing institutional website.* Bunny.net migration from Cloudflare is documented as achievable in under two hours for standard deployments, requiring a DNS record change and propagation time. No architectural rethinking, no

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

data migration, no prior contract of any complexity. The exercise builds the operational reflex for CDN switching, creates an internal reference for the process, and removes one American intermediary from the traffic path between the institution and its users. For organisations that operate multiple websites, start with the lowest-traffic one.

These four actions do not individually constitute a migration strategy. They constitute an organisation's first evidence about its own capacity to act. An organisation that has completed all four within 90 days has resolved a documented GDPR violation, reduced its software supply chain exposure, produced the document on which IAM migration planning depends, and demonstrated that provider substitution is operationally feasible at bounded scope. That is the foundation on which the planning in section 5.3 can begin.

5.3 - At six to twenty-four months: migrations to plan now

These actions require budget and planning authority. They do not require waiting for European coordination to be resolved.

Apply the matrix to the organisation's specific stack. Place each critical dependency in its quadrant. For each Quadrant 1 dependency (critical severity, accessible migration), the output names the target European alternative, the migration lead, the budget envelope, and the deadline tied to the next contract renewal. For each Quadrant 2 dependency (critical severity, difficuly migration), it names the programme owner, the multi-year horizon, and the interim risk mitigation measures. The matrix also identifies what not to prioritise: address the highest-criticality, most-accessible dependencies first, build migration competence on those successes, then apply it to harder problems in the second cycle.

Use contract renewals as the action window. At each renewal: issue a market consultation before the process begins and document the result formally, introduce the four dependency dimensions as explicit scored criteria in the procurement matrix, negotiate data portability and termination terms explicitly regardless of which provider is selected. The EU Data Act's Article 25 switching assistance obligations set a floor that contractual negotiation can raise as needed.

Pilot before committing. No large-scale migration should be initiated without a pilot on a bounded, non-critical workload. The pilot builds internal competence, produces an assessment of the European alternative's actual maturity within the organisation's specific environment, and generates a documented result that executive leadership can evaluate before committing at scale. File storage and internal messaging are the standard candidates. The pilot population should be internal users, not customer-(or public-)facing services.

Pool experience and participate in consultations. The friction costs of migration are shared problems. Organisations that have completed migrations at scale have produced transferable knowledge that most organisations attempting migration are not systematically accessing. Two mechanisms make pooling concrete: participation in national open-source communities

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

(code.gouv.fr, Open CoDE, the Interoperable Europe Portal) and coalitions of public buyers around shared procurement requirements, which create the commercial viability signal that European managed service providers need to invest in scaling. ENISA, DG CONNECT, and the Interoperable Europe Board all conduct public consultations on the standards being designed. An organisation that has encountered a specific interoperability barrier during a pilot has produced exactly the evidence those bodies need. Submitting it converts operational experience directly into the evidentiary record on which regulatory requirements are built.

5.4 - At five years and beyond: what requires coordinated European action

The four decisions that would materially change the conditions described throughout this report are documented in section 4 and consolidated in Annex G with their institutional owners, current blockers, and progress signals: establishing sovereignty criteria as binding eligibility thresholds through the CADA and sectoral mandates where the EUCS failed to carry them, mandating open interoperability protocols through the Interoperable Europe Board, establishing a joint procurement framework for sovereign digital services, and directing the DC-EDIC to define binding workload portability floors by layer. All four are achievable through institutions that already exist.

What individual organisations can do to accelerate those decisions is narrow but not negligible. A formal NIS2 Article 21 risk register that documents unresolved dependencies by name, with the American corporate entity responsible and the estimated operational impact of activation, creates the evidentiary record that regulatory bodies and elected officials need to act. A dependency documented and escalated through the correct institutional channel is not the same as a dependency that sits in a CIO's mental model and goes nowhere. The organisations that treat their dependency exposure as a governance matter rather than a technical one are the ones that produce the inputs from which policy is made.

For organisations subject to financial reporting obligations, the dependency exposure documented through this process has a governance dimension that extends beyond the IT function. Operational dependencies of the kind mapped in section 2, where a single vendor decision can halt core operations, qualify as operational risks under IFRS standards and, increasingly, under ESG reporting frameworks. The dependency audit conducted under section 5.2 serves simultaneously as NIS2 compliance documentation and as source material for a risk disclosure that belongs in the organisation's annual governance reporting. External auditors with a mandate to assess operational risk completeness should flag an undisclosed material dependency of this kind. For IT directors seeking to escalate the dependency assessment to executive or board level, the risk disclosure framing is frequently more effective than the sovereignty or cybersecurity framing: it connects to an existing governance obligation rather than requesting a new one.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Section 6 - What successful migrations look like: documented cases and transferable lessons

The prioritisation logic of section 5 is necessary but not sufficient. A decision-maker who has mapped their dependencies, identified their critical single points of failure, and placed each in the appropriate quadrant still faces a question that no matrix can answer: is this actually doable, at our scale, with our constraints, in our institutional context?

The cases that follow answer that question with evidence rather than assertion. They are not success stories selected to inspire, but rather documented cases chosen because they represent distinct combinations of institutional authority, political mandate, operational scale, and external pressure. Those four variables, more than any technical consideration, determine whether a migration succeeds, stalls, or never begins. Each case is examined for what made it work, what would not transfer to a different context, and what the organisations that attempted it would do differently.

One of the four cases did not result in a completed migration. It is included for that reason, and has equally relevant lessons to teach, though recent developments seem to indicate that the process is still alive[159].

6.1 - Large institutional migration under hierarchical authority

The Gendarmerie Nationale's GendBuntu project is the most extensively documented large-scale desktop migration in European public sector history. Its scale is unambiguous: as of June 2024, 97% of workstations run GendBuntu, covering 103,164 stations. Its financial outcome is documented: a 40% reduction in total cost of ownership, approximately €2 million in annual licence savings, and cumulative savings estimated at €50 million[160]. It is cited in almost every European sovereignty discussion as proof that migration at scale is possible. That framing is correct but incomplete. The conditions under which it succeeded are as important as the outcome, and some of them are not directly replicable in a civilian administrative context.

What actually happened, and when

The migration did not begin as a sovereignty project. It began with a financial constraint and a layer-by-layer response to it. Prior to 2005, the Gendarmerie found that spiralling licensing costs and time-consuming maintenance were placing a strain on its resources. In 2004, OpenOffice.org replaced 20,000 copies of the Microsoft Office suite, with the transfer of all 90,000 office suites completed in 2005. In 2006, migration began to Firefox on 70,000 workstations and to Thunderbird for email. The decision to migrate the operating system itself came later: in 2008, the decision was made to migrate to Ubuntu on 90% of the Gendarmerie's computers, with Ubuntu installed on 5,000 workstations primarily for training purposes. The full OS migration was substantially complete by 2014, a decade after the first application-layer decision.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The sequencing is the first transferable lesson. The Gendarmerie did not attempt to migrate the operating system and the application layer simultaneously. It standardised on open-source applications first, under Windows, which had two effects: it reduced user retraining requirements at the OS migration stage, because the daily tools were already familiar, and it identified the application compatibility blockers in advance, before the OS transition created operational pressure. Around 90% of the 10,000 computers purchased by the Gendarmerie per year were bought without an operating system, with GendBuntu installed by the Gendarmerie's technical department, allowing the migration to be absorbed progressively through the natural hardware replacement cycle rather than as a forced conversion of existing machines.

The enabling conditions

Three conditions made this migration succeed that are specific to the Gendarmerie's institutional context, and transferable only to specific other use cases.

The first is hierarchical authority. The Gendarmerie operates under military command structures. A decision taken at the appropriate level is implemented across 4,300 police stations distributed across metropolitan France and overseas territories without the negotiation, opt-out, or shadow IT proliferation that would accompany an equivalent decision in a civilian ministry. The main technical problem encountered was keeping the existing computer system online while the update took place, not only in metropolitan France but also in overseas *Départements* and *Régions,* which represents an important but purely logistical challenge. The governance problem, which is the primary failure mode in civilian migrations, did not exist.

The second is usage homogeneity. Gendarmerie workstations support a defined and relatively uniform set of operational tasks: administrative processing, communication, documentation, and access to national police information systems. There are no graphic design departments, no complex financial modelling workflows, no proprietary sector-specific applications developed over decades by external vendors. The tail of edge cases that defeats civilian migrations at the application compatibility stage was short.

The third is the absence of cloud dependency. The GendBuntu migration addressed the desktop layer entirely. It did not address identity management, cloud infrastructure, SaaS platforms, or inter-organisational collaboration at scale. In 2005, those layers did not exist in their current form. A comparable migration undertaken today would need to resolve the IAM dependency documented in section 2.2, the collaboration interoperability problem documented in section 2.4, and the application integration layer that did not exist when GendBuntu was designed. The difficulty of replication reflects the increased complexity of the dependency landscape in the twenty years since GendBuntu began, not the exceptional character of what the Gendarmerie achieved.

What transfers

The layer-by-layer sequencing method transfers directly and is the most actionable lesson for any organisation considering a migration. Standardise on open-source applications before migrating the operating system. Use the hardware replacement cycle to absorb the OS transition progressively

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

rather than converting existing machines under pressure. Invest in deep user training on a bounded pilot population before scaling: the migration began with habituation of agents to open-source software, allowing an intermediate step that reduced the impact on their daily working environment. The pilot-first logic of section 5.3 is derived directly from this sequencing.

The documentation practice also transfers. The Gendarmerie's technical leads published their methodology, their timeline, and their failure modes at public conferences throughout the migration. That documentation is a public good that subsequent migrations, including Schleswig-Holstein and the ICC deployment described in the sections that follow, drew on directly. An organisation that pilots a migration and publishes its results, including the problems it encountered, contributes to the European shared knowledge base that reduces the cost of every subsequent migration that follows the same path.

What does not transfer

The command model does not transfer to civilian administrations, and presenting the GendBuntu case as a blueprint without stating this clearly is an analytical error that has contributed to unrealistic migration planning in several European public administrations. A Director of Digital Services in a civilian ministry does not have the authority to issue a descending instruction that is implemented across every directorate without negotiation. The governance challenge that the Gendarmerie did not face is the primary challenge that civilian administrations do face, and it requires a different approach: the political mandate model described in section 6.2, rather than the hierarchical decision model that produced GendBuntu.

6.2 - Large subnational administration with political mandate

Schleswig-Holstein is the most closely watched open-source migration in European public administration today, and the most frequently misread. Its headline figures are real: almost 80% of workplaces in the state administration have been switched to LibreOffice, with annual licence savings exceeding €15 million from 2026 (and €9 million reinvested in open source development in the same year[161]), a payback period of under one year. In October 2025, the state completed its email migration, moving over 40,000 mailboxes containing more than 100 million emails and calendar entries from Microsoft Exchange and Outlook to Open-Xchange and Thunderbird, in a six-month process covering approximately 30,000 employees across the State Chancellery, ministries, judiciary, state police, and other authorities[162]. What those figures do not capture is the governance architecture that made them possible, and the difficulties that the migration encountered along the way.

What actually happened, and when

This migration did not begin as a sovereignty project either. Much like the Gendarmerie Nationale, it began as a financial and strategic assessment that reached a sovereignty conclusion. Dirk Schrödter, Head of the State Chancellery and Minister for Digital Transformation, framed the

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

rationale explicitly: administrations and businesses are trapped in a system characterised by monopolistic structures and high licensing fees, and it is a core responsibility of the state to be able to influence the operational processes of its IT systems at all times and to ensure the data security of its citizens and businesses[163]. That framing is significant: the political mandate was not constructed around a crisis but around a strategic assessment of structural dependency, and it preceded the ICC case that subsequently validated it publicly.

The sequencing followed a layer-by-layer logic comparable to the Gendarmerie model. LibreOffice was deployed as a parallel installation alongside Microsoft Office before any forced removal. ODF became the official document format for the state administration as of August 1, 2024[164], providing a structural incentive to use LibreOffice before the Microsoft licence was cancelled. Email migration followed office software standardisation. The Linux operating system migration is, at the time of writing of this report, in pilot phase, with the Chancellery itself operating a test fleet. The sequence reduced retraining requirements at each stage by ensuring that the next layer's tools were already familiar before the previous layer's fallback was removed.

The migration was not frictionless. Minister Schrödter publicly acknowledged problems in a letter to state employees[165], apologising for stressful weeks and operational issues. The opposition noted that 80% of workplaces may have been converted on paper while far fewer than 80% of employees could work with them properly, with errors in the migration still present. These are documented difficulties that any organisation planning a comparable migration should anticipate, not anomalies specific to Schleswig-Holstein.

The enabling conditions

The primary enabling condition is a named political owner with sustained authority. Dirk Schrödter has held the digital transformation portfolio continuously since the migration's acceleration, across a coalition government involving both CDU and Green ministers[166]. The commitment from both coalition partners demonstrates that digital sovereignty can function as a bipartisan objective rather than a partisan one. The migration survived a government formation that could have reset it, because the financial and strategic case had been documented publicly and the institutional momentum was sufficient to carry it through.

The second enabling condition is the public-private coordination model. Schleswig-Holstein established an Open Source Program Office to coordinate and oversee the state's open-source strategy, funding a local innovation hub where civil-society groups, universities, startups, businesses, and public sector organisations work to build a state-wide open-source ecosystem. Schrödter explicitly reframed licence savings as an investment in the domestic digital economy: "Instead of investing our IT funding in licence fees, we use it to finance development and support contracts."[167] This reframing is analytically important: it converts the migration from a cost-cutting exercise into an industrial policy decision, which changes its political valence and broadens the coalition of interests that support it.

The third enabling condition is the publication of results, including failures. The state has committed to sharing its migration tools and experiences with other regions and public

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

institutions[168], with documented interest from Denmark, the UK, France, New Zealand, India, Switzerland, and Austria. The transparency is the mechanism by which a regional migration becomes a transferable model.

What transfers

Three elements transfer directly to other institutional contexts. The parallel installation strategy, deploying the open-source alternative alongside the incumbent before removing the fallback, reduces the user disruption that makes large-scale migrations fail at the change management stage. The ODF mandate as a procurement and document exchange requirement creates a structural incentive that nudges daily behaviour before any forced migration occurs. And the public documentation of both successes and difficulties produces the shared knowledge base that reduces the cost of every subsequent migration attempting the same path.

The financial reframing also transfers, and is underused in most European public sector contexts. An organisation that presents a migration as "saving €15 million in licence fees" is making a different political argument from one that presents it as "redirecting €15 million from American licence fees to European development and support contracts".

What does not transfer

Two conditions that enabled the Schleswig-Holstein migration are not generalisable without explicit acknowledgement.

The first is budgetary capacity. A German Land has access to dedicated multi-year IT investment budgets that most European regional and municipal administrations do not. The €9 million one-time transition cost is manageable for Schleswig-Holstein. For a French département or an Italian comune of comparable administrative scale, it is a different planning conversation. The financial case is replicable in principle, but the capital availability to execute it is not uniform across European public administrations.

The second is the tradition of administrative independence. German Länder have constitutional competence over their own administrative infrastructure and a long tradition of exercising it. A comparable migration in a French ministry, where digital infrastructure decisions intersect with interministerial coordination requirements and DINUM oversight, operates in a structurally different governance environment. The political mandate model transfers but the specific institutional conditions that made it achievable in Schleswig-Holstein do not transfer automatically.

6.3 - Institution under external pressure triggering accelerated migration

The International Criminal Court is transitioning its entire digital workspace from Microsoft 365 to openDesk, a European open-source software suite, covering approximately 1,800 workstations[169]. On 31 October 2025, the Court confirmed it is replacing its Microsoft Office Suite with openDesk, open-source software developed by Germany's ZenDiS, Centre for Digital Sovereignty[170]. The

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

decision was taken not at the end of a planned migration programme but in the middle of a sanctions crisis. The ICC's Head of Digital Services stated explicitly: "Given the circumstances, we must reduce dependencies and strengthen the technological autonomy of the Court, even if this is expensive, inefficient and inconvenient in the short term".[171]

This case is the only documented instance in this report of a migration triggered by the activation of the dependency mechanism rather than by anticipation of it. Its analytical value is precisely that: it demonstrates what migration looks like when the decision is no longer discretionary.

What actually happened, and when

The triggering sequence is documented in the introduction to this report. The sanctions sequence ran from February to October 2025. By 31 October, less than three months after the emergency internal meetings of September, the Court had publicly confirmed the migration to openDesk.

Microsoft President Brad Smith denied that the company had ceased or suspended its services to the ICC, telling reporters "at no point did Microsoft cease or suspend its services to the ICC."[172]. That denial is itself analytically significant. Whether the account suspension was the result of an American corporate decision or an automated sanctions compliance process is, from an operational standpoint, irrelevant. The access was interrupted. The mechanism whose existence this report documents was activated, visibly enough to trigger an emergency migration at an international judicial institution. That legal and operational ambiguity is the environment in which the dependency described in section 2.2 operates.

The enabling conditions

Three conditions allowed the ICC to execute an accelerated migration that most organisations of comparable administrative profile could not replicate at the same speed.

The first is scale. Although the ICC is a relatively small Microsoft customer, with under 2,000 workstations[173], this is a migration scope that a determined team can manage within weeks. The same decision at a national ministry with 50,000 workstations, heterogeneous application portfolios, and inter-organisational collaboration dependencies across dozens of partner institutions is a fundamentally different operational undertaking.

The second is usage homogeneity. The ICC's workload is predominantly documentary: legal drafting, case management, communication, and file storage. Its application portfolio does not include the proprietary sector-specific systems, financial modelling environments, or engineering toolchains that dominate public sector application portfolios in larger administrations. openDesk's functional coverage (document editing, email, calendar, video conferencing, and file storage) maps directly onto that workload without requiring application-layer rethinking.

The third, paradoxically, is the external pressure itself. The institutional inertia documented in section 1.3 as the primary obstacle to sovereign migration was eliminated by the sanctions event. The question was no longer whether migration was worth the disruption. It was whether the Court

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

could continue to function without one. That reframing removed the governance obstacle that defeats most migration projects before they begin.

What transfers

One finding transfers directly and unconditionally: a migration of this scope is technically executable under time pressure. The ICC case directly contradicts the standard objection that migration is too disruptive, too slow, or too risky to execute. An institution with a manageable workstation count, a homogeneous usage profile, and a political decision to proceed can replace its Microsoft 365 environment with an operationally viable European alternative within weeks. That finding is available to any organisation that uses it to structure a planned migration before the pressure arrives, rather than as evidence that crisis migration is a reliable strategy.

The publication of the ICC migration as a confirmed, documented case also produces a secondary effect that the Schleswig-Holstein migration produced in a different register: it removes the claim that "no organisation of our type has done this" from the repertoire of arguments against migration. The ICC joins the Gendarmerie Nationale, Schleswig-Holstein, the Austrian Federal Ministry for Economic Affairs, and the German Bundeswehr in a growing reference set that procurement officers and CIOs can cite against institutional resistance.

What does not transfer

The ICC case should not be read as evidence that urgency is a sufficient condition for successful migration. It is a necessary condition for removing institutional inertia, but the ICC's specific profile (relatively small scale, homogeneous usage, and absence of complex inter-organisational integration dependencies) is not generalisable.

An expert quoted in Erasmus Magazine stated the constraint directly: "The Court has to act quickly now, under pressure, but if a university wanted to leave Microsoft tomorrow, that would cause problems."[174]. The same observation applies to any large administration with a heterogeneous application portfolio and deep inter-organisational collaboration dependencies. For those organisations, the ICC case is a proof of concept for a bounded subset of the migration problem, and treating it as more than that produces planning assumptions that will not survive contact with a real migration programme.

The more consequential lesson is the one the ICC case was designed to avoid delivering: the organisations best positioned to execute a rapid migration under pressure are those that have already conducted the dependency audit, identified the European alternatives, and piloted them on non-critical workloads before the pressure arrives. The ICC migrated quickly because the path was short. For larger organisations, shortening the path is the work of the years before the crisis, not the weeks during it.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

6.4 - Change management framework applicable to public institutions

The DGFiP is the French tax authority. Its 95,000 workstations make it one of the largest IT estates in French public administration. Between 2022 and 2024, acting as pilot of the interministerial open-source software support market, it commissioned and published a study titled *Poste de travail Linux: état de l'art et conduite du changement*.[175] The study is rigorous, methodologically sound, and published under a Creative Commons CC BY-SA 2.0 licence in OpenDocument format: a deliberate signal of intent. However, the DGFiP then deployed Windows 11 across its entire workstation fleet.[176]

What the study actually contains

The study's primary contribution is a functional arbitration matrix that classifies workloads into three categories: those that migrate to Linux without constraint, those requiring case-by-case analysis, and those that represent genuine current blockers.

The first category is larger than most organisations assume. Office productivity, communication, web browsing, PDF creation and annotation, document management, and collaborative working are all assessed as generalisable to Linux based on both theoretical evaluation and documented operational feedback. These workloads cover the daily activity of the overwhelming majority of agents in any public administration.

The second category, workloads requiring case-by-case analysis, primarily covers proprietary sector-specific business applications. The constraint here is not Linux compatibility per se but application architecture: applications built on Windows-native frameworks, dependent on Internet Explorer rendering engines, or integrated with Active Directory in ways that assume Windows as the host OS. Each of these requires an individual compatibility assessment before migration can be planned. The study provides the framework for conducting that assessment; it does not perform it for any specific administration.

The third category, genuine current blockers, is narrower than the political debate around Linux migration typically suggests. Genuine current blockers do exist but are narrower than the political debate typically suggests. They are concentrated in specialised professional workflows (certain design and engineering environments) where commercial software has no Linux-native equivalent of comparable maturity. For the overwhelming majority of public sector workloads, they are not relevant.

What the study does not contain

The study is explicitly non-prescriptive. Its authors state that it does not constitute a ready-to-use solution for a migration to Linux and that each administration must adjust its approach to its own constraints. That framing is honest but has a practical consequence: the study produces a framework for thinking about migration without producing a mandate to execute one.

The change management dimension, which the title foregrounds, is the study's most operationally useful contribution and its least developed section. It identifies user training, transition support, and

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

clear communication as key success factors. This conclusion is both correct and insufficiently specific. The Gendarmerie's experience, documented in section 6.1, provides more operational depth on what deep rather than surface training actually looks like in practice.

Why the DGFiP did not migrate, and what has changed

The operational decision is documented through union consultation records. As of the April 2025 interministerial working group on information systems, the DGFiP's 95,000 workstations are running Windows 11. The union confederations CFDT and CFTC noted explicitly that workstations rendered hardware-incompatible with Windows 11, and which the application decoupling work completed for the study would have made Linux-recyclable, are being decommissioned rather than repurposed.[177]

The DGFiP's dependency profile makes this decision the more notable. DGFiP Director of Digital Services Tomasz Blanc confirmed that the administration does not use Microsoft Office, does not use Active Directory, and orients all new projects by default toward its sovereign cloud platform NUBO, running on a fully open-source stack.[178] That profile is precisely the one the study identified as most favourable for a Linux workstation migration. The technical preconditions were met. The dependency on Windows itself had become the only remaining Microsoft foothold.

The explanation for the non-migration is institutional rather than technical. A migration of 95,000 workstations is a multi-year programme of exceptional complexity and operational risk, conducted under the full scrutiny of parliamentary oversight, trade union consultation, and public accountability. The conditions that removed that calculus at the Gendarmerie (military command authority) and at Schleswig-Holstein (sustained political mandate with named ministerial ownership) were not present at the DGFiP. The study produced a methodological framework, which was its mandate, rather than the governance conditions under which that framework could be applied.

As of the publication date of this report, that position is shifting. Blanc has stated publicly that hosting fiscal data subject to the CLOUD Act is institutionally untenable for a *régalienne* administration, and that a Linux workstation migration is under active study. The DGFiP's trajectory may therefore produce, in a subsequent edition of this report, the documented migration case that the 2024 study anticipated but did not itself generate.

What transfers

The functional arbitration matrix transfers directly and completely. Any public sector IT director can apply it to their own workload portfolio without commissioning a new study. The three-category classification (generalisable without constraint, requiring case-by-case analysis, and genuine current blocker) is the analytical tool that converts a migration from an undifferentiated organisational disruption into a sequenced programme with identifiable scope. It is the instrument that makes the pilot-first logic of section 5.3 operationally concrete: start with the workloads the matrix places in the first category, on a bounded population, before engaging with the second.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

The DGFiP case also transfers a negative lesson that is equally useful. The existence of a rigorous methodological framework is a necessary but not sufficient condition for migration. The organisations that have completed migrations at scale (the Gendarmerie, Schleswig-Holstein, the ICC) share one attribute that the DGFiP study did not produce: a governance decision at the level of authority required to execute it. The study tells you what to do, and the governance structure determines whether it gets done.

6.5 - What scales and what does not: a synthesis for different audiences

The four cases do not map uniformly onto every institutional profile. The synthesis below draws the transferable lessons for each, without flattening the differences between them.

Profile 1: Small municipal administration (up to 500 agents)

The Échirolles municipal case, documented in section 5.1, is the most directly relevant migration reference at this scale. A municipality of comparable size executed a progressive open-source migration with no dedicated capital budget, absorbing the transition through the hardware replacement cycle and internal retraining, with documented annual licence savings of approximately €350,000 on a total IT budget of €1 million. The DGFiP functional arbitration matrix is the right starting tool: at this scale, workloads are typically concentrated in the first category, office productivity, communication, web, and document management. Genuine blockers exist but are fewer than at larger scales and must be verified before any commitment is made.

The critical precondition is executive sponsorship at the level of the mayor or municipal director. The dependency audit of section 5.2 required to acquire that sponsorship is achievable by a single IT manager in days.

Realistic horizons: productivity suite and email, six to eighteen months. OS migration, twenty-four to thirty-six months, contingent on application assessment. IAM to Keycloak, achievable but to be sequenced after the productivity layer is stable.

The preconditions above assume a minimum internal IT capacity that a substantial share of small European municipalities do not have. An administration of 300 agents with a single part-time IT officer cannot deploy Keycloak, manage an artifact proxy, or run a productivity suite migration without external operational support. For this profile, the migration question is not primarily technical. It is whether a shared services model exists that can absorb the operational complexity on behalf of a group of small administrations.

Intercommunal digital syndicates in France, Zweckverbände in Germany, and shared local government IT services in the Nordic countries already operate shared infrastructure for groups of small administrations. What most of them do not yet do is operate those shared services against sovereignty criteria. Reorienting existing shared service structures toward European providers, open-source platforms, and the portability floor defined in section 4.5 would extend viable migration options to small administrations without requiring each one to build internal capacity it

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

will not have. The investment required is in the shared service operator, not in each individual administration. The financial and operational returns accrue across the group.

The associations federating small administrations at national level, including the AMF in France and the DStGB in Germany, have the convening authority to aggregate demand across hundreds of administrations, the procurement legitimacy to negotiate with European providers at scale, and the communication channels to reach the elected officials whose political commitment is the enabling condition for any migration at this scale. This is the organisational model through which the prescriptions of this report become accessible to the largest segment of European public administration by number of entities.

Profile 2: Regional administration (up to 5,000 agents)

The Schleswig-Holstein model is the primary reference at this scale, with the budget caveat stated in section 6.2. Layer-by-layer sequencing, ODF mandate ahead of forced migration, parallel installation, and the reframing of licence savings as investment in domestic development contracts all transfer directly. The DGFiP matrix applies with greater operational weight here: proprietary sector-specific applications are more likely, and the case-by-case analysis they require is more resource-intensive than at municipal scale.

The binding precondition is a named political owner with a mandate that survives the electoral cycle. Without it, the migration stalls at the pilot phase for the reasons documented in section 1.3.

Realistic horizons: productivity suite and email, twelve to twenty-four months. IAM, eighteen to thirty-six months. Cloud infrastructure for core workloads, within two procurement cycles if European providers are introduced at the next renewal. Full Linux desktop, three to five years contingent on application portfolio assessment.

Profile 3: Ministry or large national agency (50,000 agents and above)

The Gendarmerie model is the only documented case at this scale. Its transferable lesson is the sequencing method: application layer first, OS layer second, absorbed through the hardware replacement cycle. Military command authority does not transfer.

At this scale, inter-organisational collaboration is the hardest problem. A ministry that migrates its internal productivity stack still participates in Teams calls with every partner ministry, contractor, and agency that has not migrated. The coalition logic of section 5.3 is the only mechanism through which that layer can be addressed, and it is not optional.

The binding preconditions are a governance structure with authority over all affected directorates and a dedicated programme management office resourced for the full migration horizon. The DGFiP case established that methodological rigour without those conditions produces a study but not necessarily a migration.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Realistic horizons: productivity suite pilot on a subset of directorates, twenty-four to thirty-six months. Full deployment, four to six years. IAM, three to five years with parallel Keycloak operation throughout. Full Linux desktop, five to ten years.

What the cases establish collectively

The cases in this section are presented as evidence rather than models. The Gendarmerie and Schleswig-Holstein cases establish that large-scale migration is feasible and financially positive. The ICC case establishes that accelerated migration is technically executable when the governance obstacle is removed. The DGFiP case establishes that methodological readiness without governance authority produces no operational outcome.

Together, they locate the primary binding constraint: not technical capacity, but the ecosystem of incentives, standards, and coordination mechanisms that shapes procurement decisions across thousands of organisations simultaneously. The four decisions that individual organisations cannot activate are documented in section 4. Annex G consolidates them with their institutional owners, current blockers, and progress signals.

CONCLUSION: EUROPE'S DIGITAL INFRASTRUCTURE, ON EUROPEAN TERMS

A - What this report has established

Three things, and three only.

The first is that digital dependency on American technology platforms creates operational, jurisdictional, economic, and normative exposure for European public organisations simultaneously, in ways that are not always visible until a crisis activates them. That exposure is not uniform. It is concentrated in specific layers, and the mapping in section 2 identifies precisely which ones.

The second is that the information environment surrounding this dependency has been systematically distorted. Structural incentives reward the status quo, and the actors who benefit from it have invested accordingly: in lobbying at record scale, in consultant incentive structures aligned with incumbent platforms, and in procurement architectures that make alternatives administratively invisible. Whether any individual actor acted in bad faith is operationally irrelevant. The aggregate outcome is a collective dependency that deepens with every procurement cycle, and that no individual actor on the receiving end can resolve alone.

The third is that the dependency is not a fatality. The majority of European public organisations have more migration options available to them today than the prevailing narrative suggests, and the conditions for acting on those options are more favourable now than at any point in the past decade.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

B - The right frame

The debate on European digital sovereignty has been conducted in the wrong frame for twenty years. The question has been "how do we build a European equivalent of AWS?" That question has no satisfactory answer, and asking it has produced twenty years of initiatives that measured European ambition against American incumbents as the reference point and found it wanting.

The right frame is different. Europe does not need to replicate what American hyperscalers built. It needs to architect a digital infrastructure that is fit for European companies and public institutions, built on European providers, governed by European law, and interoperable by design. That objective is achievable, as demonstrated by the several organisations documented in this report that are already achieving it.

Europe's actual strengths in this domain are real and underexploited. A deep and skilled open-source culture encompassing all sectors. Technically excellent, specialised providers across every layer of the stack. A regulatory capacity that is the most powerful in the world and that can function as a sovereignty instrument rather than merely a compliance burden. And a structural heterogeneity that is simultaneously a coordination liability and a resilience asset: no single point of failure, no single jurisdiction, no single point of political leverage.

The fragmentation that is most frequently cited as Europe's competitive weakness relative to American hyperscalers is, under the full rupture scenario examined in section 3, its most durable structural advantage. Preserving that heterogeneity while building the interoperability layer that makes it function as a coherent offering is the architectural challenge. It is a more tractable challenge than trying to build a European AWS.

This framework applies beyond the public sector. The GDPR, the CLOUD Act's jurisdictional reach, and the dependency mechanisms documented throughout this report do not distinguish between a ministry and an industrial group. The analytical framework of section 2 and the prioritisation logic of section 5 are directly applicable to any European organisation of significant scale. The public sector is the primary audience of this report because its obligations are the most explicit and its accountability the most immediate. It is not the only constituency with a material interest in the outcome.

C - How the dependencies were created

This report would be incomplete without acknowledging the role of European institutions and member states in creating the conditions it documents. The dependencies mapped here did not emerge in spite of European policy. They emerged in significant part because of procurement decisions made at every level of European public administration over twenty years: decisions that chose American platforms for reasons of convenience, cost, and the absence of credible alternatives at the time, and that were subsequently locked in by the same switching costs this report describes.

This is a diagnosis, not a prosecution: vendor lock-in strategies, consultant incentive structures, and the individual risk calculus of IT decision-makers each played a predictable role. These were

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

predictable outcomes of predictable incentive structures. The path forward does not require exhorting individuals to act against their rational self-interest. It requires changing the incentive structures themselves: procurement frameworks that treat sovereignty criteria as eligibility thresholds, investment that gives European vendors the scale to compete, and interoperability mandates that reduce the switching costs that currently make single-vendor American architectures artificially attractive.

D - The window, and what to do with it

Something has shifted. Not decisively, not irreversibly, but measurably.

Wero has more than 43.5 million registered users and live merchant payments in Germany. Schleswig-Holstein has completed its email migration and documented a payback period of under one year. The Austrian Armed Forces removed Microsoft Office from all 16,000 military workstations in September 2025, citing digital sovereignty as the primary driver. Denmark's Ministry of Digital Affairs announced a transition to Linux and LibreOffice in June 2025. The Dutch parliament voted to accelerate investment in European cloud alternatives after the Solvinity acquisition threatened to place national citizen authentication infrastructure under American corporate control. The ICC migrated to openDesk within weeks of dependency activation. The Franco-German summit of November 2025 produced the most explicit bilateral political commitment to European digital sovereignty in a decade, and the DC-EDIC is operational with four founding member states.

Finland's Security and Intelligence Service has explicitly stated that dependence on foreign cloud providers could undermine sovereignty, prompting the Ministry of Justice to remove election data from Amazon Web Services. In February 2026, German Chancellor Friedrich Merz stated at the Munich Security Conference that Europe's excessive dependency on the United States was "self-inflicted." In January 2026, the European Parliament voted 471 to 68 for a resolution on European technological sovereignty, with support from every major political group. The signal is no longer confined to any single member state or political tendency.

None of this resolves the dependency map of section 2. What it represents is the beginning of the conditions under which that map can be changed: political will forming at the level where the collective action problem can be addressed, market alternatives reaching production maturity at the layers where migration is most accessible, and a reference set of completed migrations that removes the claim that "no organisation of our profile has done this" from the repertoire of arguments against acting.

The public sector is the primary audience of this report because its accountability is the most immediate and its obligations the most explicit. However, the same dependency mechanism documented in the introduction, the same CLOUD Act jurisdiction, the same IAM single point of failure, the same payment network exposure, applies without modification to European banks, insurers, hospital groups, energy utilities, and operators of critical infrastructure, whether publicly or privately governed. The difference is that public administrations face electoral accountability for

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

governance failures while private sector boards face shareholder and audit committee accountability.

The asymmetry documented in section 2.7 runs in both directions. The AI dependency being created today will be harder to unwind in five years than the cloud dependency of 2015 is today. But the infrastructure decisions taken today, the pre-contracted European IaaS environment, the parallel Keycloak deployment, the ODF mandate, the pilot migration on a bounded workload, will be exponentially more valuable in a crisis than the same decisions taken under pressure. The organisations best positioned to act quickly when conditions require it are those that have already begun.

The ICC's Head of Digital Services described the migration as « expensive, inefficient and inconvenient in the short term. » and yet the Court completed it in weeks. That is not a counsel of fear, it is a proof of what is possible when the decision is taken.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ANNEXES

ANNEX A - Glossary of technical terms for non-specialist readers

This glossary defines the technical terms used in this report in the order most useful for a non-specialist reader. Terms that are defined in the methodological note, such as the four dependency dimensions, are not repeated here.

Active Directory A directory service developed by Microsoft for managing users, devices, and access policies within an organisation's internal network. Active Directory handles domain-joined machine authentication, group policy enforcement, and trust relationships between organisational units. It is distinct from Microsoft Entra ID (its cloud-based successor), though the two are frequently deployed together. Organisations running Active Directory without Entra ID have a different dependency profile from those running both. FreeIPA and Samba AD are the open-source alternatives for this layer. Documented in section 2.2.

AI coding assistant A software tool integrated directly into a developer's code editor (IDE) that provides context-aware code completion suggestions, generation, and explanation in real time. Unlike a general-purpose LLM accessed via a web interface, a coding assistant operates within the development environment and has continuous access to the code currently being written, the surrounding file, and in some implementations the broader repository context. This access pattern means that code content, including variable names, data structures, business logic, and comments, is transmitted to the provider's inference infrastructure with each completion request. GitHub Copilot, the dominant product in this category, routes this context through Microsoft's infrastructure; European alternatives such as Continue.dev and Tabby can be configured to route requests to self-hosted inference endpoints instead, eliminating the external data transmission. Documented in section 2.8.

ANSSI (Agence nationale de la sécurité des systèmes d'information) The French national cybersecurity agency, responsible for the SecNumCloud certification framework and for NIS2 supervision in France. ANSSI operates the MonEspaceNIS2 portal for entity registration and MonAideCyber for initial diagnostic assessment.

API (Application Programming Interface) A defined interface through which two software systems communicate. When a vendor makes a service available only through a proprietary API, any other software built to use that service becomes dependent on the vendor's decisions about how that interface operates and whether it remains available. Proprietary APIs are one of the primary mechanisms through which architectural lock-in is created.

Artifact proxy / artifact repository An internal server that caches copies of software packages downloaded from external registries such as npm, PyPI, or Docker Hub. Rather than pulling

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

packages directly from American-controlled registries at build time, a development pipeline pulls from the internal cache. This reduces both the jurisdictional exposure and the supply chain integrity risk that comes with direct dependency on external registries.

Authentication / identity provider (IdP) Authentication is the process of verifying that a user is who they claim to be. An identity provider is the system that performs this verification and issues the credential that other systems accept. In an enterprise context, the identity provider is the control plane of all digital access: every system a user touches checks with the identity provider before granting entry. Microsoft Entra ID and Keycloak are both identity providers.

Bare-metal infrastructure Physical server hardware rented directly, without a virtualisation layer managed by the provider. An organisation running workloads on bare-metal infrastructure at a European provider has a cleaner separation from the provider's managed services layer and from the jurisdictional exposure that comes with deeply integrated platform services.

BSI (Bundesamt für Sicherheit in der Informationstechnik) The German federal cybersecurity agency, responsible for the C5 cloud security certification and for NIS2 supervision in Germany.

C5 (Cloud Computing Compliance Criteria Catalogue) The German federal cloud security certification framework administered by the BSI. C5 serves a comparable function to SecNumCloud in France: a standardised, audited assurance framework for cloud service providers.

CADA (Cloud and AI Development Act) A forthcoming European regulation expected to establish EU-wide eligibility requirements for cloud service providers in public procurement, alongside measures to strengthen European cloud and AI infrastructure capacity. Expected to be proposed by the Commission in the first half of 2026.

CDN (Content Delivery Network) A geographically distributed network of servers that delivers web content to users from the server closest to them, reducing latency. CDN providers also typically offer DDoS protection and DNS resolution. Cloudflare is the dominant global CDN provider.

CI/CD (Continuous Integration / Continuous Delivery) The automated pipeline through which software code is tested, assembled, and deployed. A CI/CD pipeline typically pulls software packages from external registries at build time, creating the package registry dependency documented in section 2.8.

CLOUD Act The Clarifying Lawful Overseas Use of Data Act, adopted by the United States Congress in 2018. It compels any U.S.-incorporated company to produce data stored anywhere in the world when served with a valid U.S. government demand, regardless of where that data is physically located or whether its disclosure would violate the laws of the country in which it is stored. There is no carve-out for data stored in EU data centres and no exception for GDPR.

CNIL (Commission nationale de l'informatique et des libertés) The French national data protection authority, responsible for GDPR enforcement in France. Referenced in this report primarily in relation to the Health Data Hub authorisation on Microsoft Azure.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Container / Docker / Kubernetes A container is a standardised unit of software that packages code and its dependencies together, allowing it to run consistently across different computing environments. Docker is the dominant container format. Kubernetes is the dominant system for orchestrating large numbers of containers across a cluster of servers. Docker Hub is the primary registry from which container images are downloaded, and is operated by an American company.

DC-EDIC (Digital Commons European Digital Infrastructure Consortium) A consortium established in July 2025 by Germany, France, Italy, and the Netherlands to jointly develop and scale sovereign digital tools, including open-source alternatives for public sector productivity and collaboration. The DC-EDIC's statutory mandate covers cross-border open-source digital infrastructure development. OpenDesk, the open-source office suite adopted by the ICC and Schleswig-Holstein, was developed under its auspices.

DDoS (Distributed Denial of Service) An attack that attempts to make a website or service unavailable by overwhelming it with traffic from a large number of sources simultaneously. DDoS protection services absorb and filter this traffic before it reaches the target infrastructure.

DINUM (Direction interministérielle du numérique) The French interministerial directorate for digital affairs, responsible for coordinating the digital transformation of French public administration. DINUM maintains the SILL (Socle Interministériel de Logiciels Libres), a catalogue of 530 open-source tools recommended for French public administration.

DMA (Digital Markets Act) A European Union regulation designating large technology platforms as "gatekeepers" and imposing obligations on them, with fines of up to ten percent of global annual turnover for non-compliance and structural remedies available for repeated infringement. Referenced in section 4.7 as an enforcement instrument relevant to the dependencies documented in this report.

DNS (Domain Name System) The system that translates human-readable web addresses, such as europa.eu, into the numerical IP addresses that computers use to locate each other. DNS resolution is a foundational layer of internet connectivity: an organisation that loses control of its DNS entries loses the ability to direct traffic to its services. DNS providers can also observe every domain lookup made by users of their resolver, creating a visibility dependency.

DORA (Digital Operational Resilience Act) A European Union regulation establishing cybersecurity and operational resilience requirements for financial institutions, including banks, insurers, and investment firms. DORA imposes obligations on ICT third-party risk management that are directly relevant to the dependencies documented in this report for any financial sector entity.

EDR (Endpoint Detection and Response) A security platform deployed on individual workstations, servers, and devices that monitors for malicious activity at the operating system level in real time. EDR platforms typically operate at kernel level, giving them access to process activity, file operations, network connections, and user behaviour. This deep integration is what makes EDR effective and what makes the choice of EDR vendor a sovereignty-relevant decision.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

eIDAS 2.0 The revised European regulation on electronic identification and trust services, adopted in 2024. It establishes the framework for the European Digital Identity Wallet, a standardised digital identity credential that EU citizens can use for authentication across member states. Its primary scope is citizen-facing authentication; the equivalent standard for machine-to-machine and administrative B2B authentication does not yet exist at European scale.

ENISA (European Union Agency for Cybersecurity) The EU agency responsible for cybersecurity policy support, including the development of the EUCS certification framework and the publication of NIS2 technical implementation guidance mapping NIS2 requirements to ISO/IEC 27001:2022 and NIST CSF 2.0.

ENS (Esquema Nacional de Seguridad) The Spanish national security framework maintained by the Centro Criptológico Nacional (CCN). ENS requirements are mapped to NIS2 in ENISA's technical implementation guidance and serve a comparable function to SecNumCloud and C5 in the Spanish context.

EUCS (European Cybersecurity Certification Scheme for Cloud Services) A harmonised European cloud security certification framework under development. The central policy question documented in section 4.1 is whether the highest assurance tier of the EUCS will include sovereignty requirements (protection against extraterritorial jurisdiction, European ownership conditions) or remain a purely technical security certification.

EuroHPC (European High Performance Computing Joint Undertaking) An EU joint undertaking that operates supercomputers across Europe for scientific research. The InvestAI initiative extends this infrastructure to include AI gigafactories for commercial AI training and inference. Referenced in section 4.7 as a vehicle for shared sovereign compute.

Extraterritorial jurisdiction The legal reach of a sovereign authority beyond its own territorial borders. The CLOUD Act is the primary operative instrument of American extraterritorial jurisdiction over data for the purposes of this report. European organisations whose data is processed by U.S.-incorporated companies are subject to American extraterritorial jurisdiction regardless of where that data is physically stored.

FedRAMP The Federal Risk and Authorization Management Program, a U.S. government framework that pre-authorises cloud services for federal procurement. A cloud provider that obtains FedRAMP authorisation has undergone a single security assessment that is accepted by all federal agencies, eliminating the need for per-agency review. This report recommends a comparable pre-qualification catalogue for European public sector procurement.

FISA (Foreign Intelligence Surveillance Act) United States legislation authorising surveillance of foreign nationals for intelligence purposes. Section 702 of FISA allows the U.S. government to compel American technology companies to provide access to communications of non-U.S. persons stored on their infrastructure. Unlike the CLOUD Act, FISA does not require a court order for each individual target. Referenced alongside the CLOUD Act as a source of jurisdictional exposure for European organisations using American platforms.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Forgejo A community-governed, open-source code hosting platform, developed under European non-profit governance (Codeberg e.V., Germany). Licensed under the GNU General Public Licence. Forgejo is the strongest sovereignty story in the code hosting layer: European governance, copyleft licence, non-profit structure. It powers Codeberg, Germany's non-profit public code hosting platform. Documented in section 2.8.

GDPR (General Data Protection Regulation) The European Union's data protection regulation, in force since 2018. GDPR establishes rules on the processing of personal data, including restrictions on transfers to jurisdictions without adequate data protection. GDPR Article 48 requires a formal international agreement as the basis for any foreign court order to compel data disclosure, a requirement that creates a direct legal conflict with the CLOUD Act in the absence of a US-EU executive agreement.

Google Play Integrity API A proprietary attestation service operated by Google that determines whether a mobile application is running on a device certified by Google, with an approved operating system and unmodified Play Services. Banking, payment, and government applications on Android typically require a passing integrity check before they will execute. The API is available exclusively on devices running Google's proprietary Android variant with Google Play Services installed. Alternative operating systems, including those based on the Android Open Source Project without Google's proprietary layer, are structurally excluded from receiving a passing attestation regardless of the security properties of the underlying device. This creates a dependency that sits below the payment or application layer and is not addressed by any currently deployed European payment sovereignty initiative. Documented in section 2.5.

GPU (Graphics Processing Unit) Originally designed for rendering images, GPUs are now the primary hardware used for training and running artificial intelligence models, because their architecture is optimised for the parallel mathematical operations that AI workloads require. NVIDIA is the dominant GPU manufacturer for AI applications. The dependency of European AI infrastructure on American-designed GPUs is documented in sections 2.7 and 3.3.

IaaS (Infrastructure as a Service) The provision of computing resources, storage, and networking as a service, without the customer managing the physical hardware. AWS EC2, OVHcloud, and Hetzner are all IaaS providers. IaaS is the foundational layer on top of which PaaS and SaaS services are built.

IAM (Identity and Access Management) The set of policies, processes, and technologies that control who can access what within an organisation's digital infrastructure. IAM encompasses authentication, authorisation, single sign-on, multi-factor authentication, and access control policy. It is described in section 2.2 as the control plane of the entire digital infrastructure.

IPI (International Procurement Instrument) A European Union regulation (EU 2022/1031) that allows the Commission to restrict access to European public procurement markets for suppliers from countries that do not offer reciprocal access to European companies. The American federal technology procurement market is substantially closed to European suppliers in categories directly

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

relevant to this report. The IPI has not been activated against the United States in any technology category as of the date of this report. Documented in section 4.7.

Interoperable Europe Act / Interoperable Europe Board A European regulation (EU 2024/903) establishing a governance framework for cross-border interoperability of public services across EU member states. The Interoperable Europe Board, which held its first operational meeting in December 2024, has the mandate to issue binding interoperability assessment guidelines. Section 4.2 of this report identifies the Board as a vehicle for mandating open protocol standards (Matrix, ODF, OpenID Connect) for public sector communication and document exchange.

Keycloak An open-source identity and access management platform, originally developed by Red Hat and now governed by the Cloud Native Computing Foundation. Keycloak supports SSO, OAuth 2.0, OpenID Connect, SAML 2.0, and multi-factor authentication. It is the primary European-origin alternative to Microsoft Entra ID documented in this report.

Kernel / kernel-level access The kernel is the core of an operating system: it manages hardware resources and mediates between hardware and software. Kernel-level access means a programme runs with the highest possible system privileges, before the operating system's normal security controls apply. EDR platforms require kernel-level access to be effective. The July 2024 CrowdStrike outage demonstrated what kernel-level access means in practice: a faulty update to a kernel driver crashed 8.5 million Windows systems simultaneously.

LLM (Large Language Model) An artificial intelligence model trained on large volumes of text data to generate, summarise, translate, and analyse text. GPT-4, Claude, Gemini, and Mistral are all large language models. The dependency of European public sector AI adoption on American LLM APIs is documented in section 2.7.

Managed service A service in which a provider handles the operational complexity of running a technology on behalf of the customer: deployment, configuration, updates, monitoring, and support. A managed Keycloak service, for example, provides the functionality of Keycloak without requiring the customer to operate the underlying infrastructure. The gap between the technical availability of European open-source alternatives and the availability of managed service wrappers around them is a recurring theme in section 2.

Matomo An open-source web analytics platform, self-hostable on European infrastructure, that serves as the primary European alternative to Google Analytics. Replacing Google Analytics with a self-hosted Matomo instance is identified in section 5.2 as the most immediately actionable migration: it closes a documented GDPR violation, costs nothing, and can be completed in days.

Matrix protocol An open, decentralised communication protocol for instant messaging and voice and video communication. Matrix allows users on different servers to communicate with each other without either server controlling the other's data, in the same way email allows communication across different email providers. France's Tchap, Germany's BundesMessenger, and the Bundeswehr's BwMessenger are all built on the Matrix protocol.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

NIS2 (Network and Information Security Directive 2) The revised European Union directive on cybersecurity, adopted in 2022 and transposed into national law by member states in 2024. NIS2 significantly expands the scope of organisations subject to mandatory cybersecurity requirements, introduces personal liability for management bodies that fail to oversee cybersecurity risk management under Article 20, and establishes incident reporting obligations. It is the primary legal vehicle through which dependency exposure should be formally documented and escalated.

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) An American cybersecurity framework widely adopted by European organisations as a risk management baseline. Organisations that have structured their security posture around NIST CSF face a real but finite gap when moving toward European frameworks. ENISA's Technical Implementation Guidance provides explicit mappings between NIST CSF 2.0 and NIS2 requirements.

npm / PyPI / Docker Hub The primary package registries for JavaScript (npm), Python (PyPI), and container images (Docker Hub) respectively. These registries are the upstream source from which the overwhelming majority of open-source software dependencies are pulled during software development and deployment. npm is operated by GitHub, a Microsoft subsidiary. PyPI is operated by the Python Software Foundation, a U.S.-based non-profit. Docker Hub is operated by Docker Inc., a U.S. company.

ODF (Open Document Format) An open, ISO-standardised file format for office documents, including text documents (.odt), spreadsheets (.ods), and presentations (.odp). ODF is the native format of LibreOffice and Collabora Online. Several European member states have mandated ODF as the standard format for public sector document exchange. Schleswig-Holstein's ODF mandate, adopted ahead of its Microsoft Office migration, is documented in section 6.2 as a key change management instrument.

OpenDesk An open-source office and collaboration suite developed under the auspices of Germany's Centre for Digital Sovereignty (ZenDiS) and the DC-EDIC. Built on Nextcloud and Collabora Online. Adopted by the International Criminal Court in November 2025 and deployed across Schleswig-Holstein's 30,000-workstation migration. Documented in sections 1.4 and 6.2.

OpenID Connect / SAML 2.0 Open protocols for identity federation: they allow a user authenticated by one identity provider to be recognised and granted access by systems managed by another organisation without creating a separate account. OpenID Connect is the more modern of the two; SAML 2.0 is more widely deployed in enterprise environments. Inter-organisational authentication across European public administrations currently depends on these protocols.

SaaS (Software as a Service) Software delivered over the internet as a subscription service, without the customer installing or managing the underlying application. Microsoft 365, Google Workspace, and Salesforce are SaaS products. SaaS creates a dependency that combines operational, jurisdictional, and economic dimensions: the customer does not control the software, the data is processed on the provider's infrastructure, and switching requires migrating data and retraining users.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

SecNumCloud The cloud security certification framework developed by ANSSI, the French national cybersecurity agency. SecNumCloud 3.2 is the most demanding cloud security certification in Europe, covering 276 requirements across 15 chapters including explicit protection against extraterritorial laws. It is the reference standard for the French public cloud doctrine and the natural reference architecture for the highest EUCS assurance tier discussed in section 4.1.

SEPA (Single Euro Payments Area) The European framework for standardised bank transfers across participating countries. SEPA credit transfers and SEPA Instant Credit Transfers are processed through European clearing infrastructure with no American intermediary in the transaction chain. SEPA Instant, which settles transactions in under ten seconds, became mandatory for all eurozone banks in January 2025.

SILL (Socle Interministériel de Logiciels Libres) A catalogue of open-source software tools recommended for use in French public administration, maintained by DINUM since 2013. The SILL references 530 tools as of 2025. Referenced in section 1.3 as one of several European initiatives that catalogue available alternatives without providing the criticality-ranked dependency assessment this report is designed to complement.

Single Sign-On (SSO) A mechanism that allows a user to authenticate once and be granted access to multiple systems without re-entering credentials for each one. SSO is typically provided by an identity provider and is a core function of enterprise IAM platforms.

SLA (Service Level Agreement) A contractual commitment by a service provider specifying measurable performance guarantees: availability (uptime percentage), response time, support response windows, and penalties for non-compliance. The absence of SLA-backed European managed services for several open-source alternatives is identified in this report as a barrier to public sector adoption.

SOC 2 (Service Organization Control 2) An American auditing standard for service providers, developed by the American Institute of Certified Public Accountants. SOC 2 reports assess controls relevant to security, availability, processing integrity, confidentiality, and privacy. Widely used by European organisations as a proxy for vendor trustworthiness in procurement, creating a normative dependency on American assurance frameworks. The European equivalents are SecNumCloud, C5, and ENS.

Sovereignty-washing The practice of adopting the language of digital sovereignty in marketing or governance frameworks while maintaining the dependencies that sovereignty is intended to eliminate. The term entered European policy vocabulary in the context of Gaia-X, where American hyperscalers joined the initiative and progressively diluted its original purpose. It is applied in section 1.5 to cloud products marketed as sovereign that retain unresolved exposure to American extraterritorial jurisdiction.

TCO (Total Cost of Ownership) The full cost of a technology over its lifecycle, including licence fees, implementation, training, support, and eventual migration. TCO analysis is used in sections

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

5.1 and 6.1 to compare the financial case for migration against the cost of continued dependency, including the cost of deferred migration under crisis conditions.

Telemetry Data automatically collected from systems and sent to a central location for analysis. EDR platforms generate telemetry by continuously monitoring endpoint activity and sending process trees, file operations, network connections, and security events to the vendor's cloud infrastructure for threat analysis. The routing of this data through American cloud infrastructure subject to the CLOUD Act is identified in section 2.3 as a jurisdictional exposure at the deepest layer of the IT stack.

VPN (Virtual Private Network) An encrypted network tunnel that allows a user to access an organisation's internal network securely from an external location. VPN access typically requires authentication through the organisation's identity provider, which means that an IAM failure also disables remote access for all users.

Wero A European digital payment solution developed by the European Payments Initiative (EPI), a consortium of European banks. Wero enables instant person-to-person and merchant payments through the SEPA Instant infrastructure, with no American intermediary in the transaction chain. With over 43.5 million registered users as of early 2026, Wero is the most advanced European initiative to reduce dependency on Visa and Mastercard payment networks. Documented in section 2.5.

XDR (Extended Detection and Response) An evolution of EDR that integrates telemetry from multiple security layers, including endpoint, network, email, and cloud, into a unified detection and response platform. Sekoia.io and Tehtris are European XDR providers documented in section 2.3.

Zero Trust A security architecture based on the principle that no user or device should be trusted by default, even within the organisation's own network perimeter. Zero Trust architectures require continuous verification of identity and device health for every access request, rather than assuming that anything inside the network boundary is safe. Cloudflare and Microsoft are among the dominant providers of Zero Trust networking products.

ANNEX B - Sources and methodology

Source selection and hierarchy

This report privileges primary sources over secondary ones throughout. Institutional publications, official regulatory documents, parliamentary records, company annual reports, and certified technical documentation are cited in preference to press summaries or analyst commentary. Where press sources are used, they are cited for documented facts, direct quotes, or confirmed event timelines, not for interpretive claims. Where a claim is analytically derived rather than directly sourced, this is stated explicitly in the text or in the relevant endnote. Sources that could not be

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

verified with sufficient precision are not cited: where a figure or claim appears without a source reference, it reflects a judgment that the available sourcing was insufficient to meet the standard applied throughout.

Evaluation of European alternatives

Every provider assessed in this report, American or European, is evaluated against the same criteria: operational maturity at production scale, documented deployment in comparable organisational contexts, and an identification of capability gaps relative to the incumbents they are compared against. European alternatives are not assessed charitably because they are European. Several are assessed as not yet viable for specific workload profiles, and those assessments are stated without qualification. This report has no commercial relationship with any vendor cited, has received no financial contribution from any technology provider, and was not shared with any vendor prior to publication.

Scope, limits, and date of information

This report covers the technology layers for which dependency on American actors creates a documented operational risk for European public organisations. The exclusions from scope, vertical sector analysis, submarine cable physical infrastructure, hardware and semiconductor supply chains, and normative dependency on American standards frameworks, are each explained in the methodological note preceding section 1. The information in this report reflects the state of the market, regulatory environment, and documented migrations as of March 2026. The European digital sovereignty landscape is moving rapidly: provider capabilities, certification statuses, and political commitments documented here should be verified against current sources before being used as the basis for procurement decisions.

1 Executive Order 14203, "Imposing Sanctions on the International Criminal Court," 6 February 2025, *Federal Register*, Vol. 90, No. 28. Available at: https://www.federalregister.gov/documents/2025/02/11/2025-02543/imposing-sanctions-on-the-international-criminal-court

2 Congressional Research Service, *Cross-Border Data Sharing Under the CLOUD Act*, Report R45173, April 2018, https://crsreports.congress.gov/product/pdf/R/R45173. CMS Law, "White Paper: Demystifying the Debate on the US CLOUD Act vs. European/UK Data Sovereignty in the Context of Cloud Services," February 2026, https://cms-lawnow.com/en/ealerts/2026/02/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data-sovereignty-in-the-context-of-cloud-services. The procedural architecture of the CLOUD Act has not, as of the date of this report, been used to compel production of enterprise data held by a European public institution on EU-based infrastructure.

3 White House, "Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties," Presidential Memorandum, 21 February 2025. Available at: https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/

4 Trump, Donald J., Truth Social post, 5 September 2025, threatening a Section 301 investigation following the European Commission's €2.95 billion antitrust fine against Google. Reported by CNN, https://www.cnn.com/2025/09/05/tech/google-eu-antitrust-fine-adtech; CNBC, https://www.cnbc.com/2025/09/05/trump-threatens-trade-probe-after-discriminatory-eu-fines-against-google-apple.html; Euronews, https://www.euronews.com/my-europe/2025/09/06/trump-threatens-retaliation-after-eu-hits-google-with-antitrust-fine

5 U.S. Department of State, statement by Secretary Marco Rubio, 23 December 2025. Reported by CNN, https://www.cnn.com/2025/12/23/politics/sanctions-censorship-state-rubio; CBC, https://www.cbc.ca/news/world/europe-france-united-states-visa-ban-9.7027301; Euronews,

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

https://www.euronews.com/my-europe/2025/12/24/us-visa-ban-targets-former-eu-commissioner-breton-over-alleged-social-media-censorship. Former Commissioner Breton and four other European citizens were barred from entering the United States for their roles in implementing the Digital Services Act and related content moderation enforcement.

6 European Union Agency for Cybersecurity (ENISA), *NIS2 Technical Implementation Guidance: Mapping to ISO/IEC 27001:2022 and NIST CSF 2.0*, version 1.0, June 2025. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

7 Bundesamt für Sicherheit in der Informationstechnik (BSI), *NIS2-Umsetzungsgesetz (NIS2UmsuCG)*, in force 6 December 2025, BGBl. 2025 I Nr. 301. Registration: https://meinunternehmenskonto.de

8 https://monespacenis2.cyber.gouv.fr/

9 https://monaide.cyber.gouv.fr/

10 Real Decreto 311/2022, *Esquema Nacional de Seguridad (ENS)*, Boletín Oficial del Estado, 10 May 2022, as mapped in ENISA Technical Implementation Guidance, Annex I.

11 European Union Agency for Cybersecurity (ENISA), *Subsea Cables - What Is at Stake?*, July 2023, ISBN 978-92-9204-612-5, DOI 10.2824/212261. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20at%20stake%20report.pdf

12 Mario Draghi, "The Future of European Competitiveness," European Commission, September 2024, Part B, pp. 183-214. Available at: https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

13 Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 (European Chips Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1781

14 Bloomsbury Intelligence and Security Institute, Digital Sovereignty and Defence Dependencies in Europe, 11 March 2026. The report documents the "dual-track" approach observed across European member states, in which civilian administrations pursue migration to European alternatives while defence establishments prioritise operational continuity through sovereign-wrapper arrangements. Available at: https://bisi.org.uk/reports/european-tech-sovereignty-and-the-security-risks-of-decoupling

15 Shapiro, Carl, and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business School Press, 1999), Chapter 5: "Lock-In." The authors document seven categories of switching costs in information markets (including durable purchases, training, data formats, and supplier-specific standards) and show that firms in these markets systematically invest in deepening lock-in as a competitive strategy, not as a neutral by-product of product development.

16 Rochet, Jean-Charles, and Jean Tirole, "Platform Competition in Two-Sided Markets," *Journal of the European Economic Association*, Vol. 1, No. 3 (June 2003), pp. 990-1029. Nobel laureate Tirole's foundational analysis of how platform operators deliberately structure pricing and access policies to exploit network effects and maximise switching costs.

17 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (Data Act), Recital 86 and Article 25. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854 ; European Commission, "Cloud Computing Policy," digital-strategy.ec.europa.eu, updated 2024, Available at: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

18 Corporate Europe Observatory and LobbyControl, "Big Tech Lobby Budgets Hit Record Levels," 29 October 2025. Available at: https://corporateeurope.org/en/2025/10/big-tech-lobby-budgets-hit-record-levels ; reported also by Euronews, "Big Tech spending on Brussels lobbying hits record high," 29 October 2025, Available at: https://www.euronews.com/next/2025/10/29/big-tech-spending-on-brussels-lobbying-hits-record-high-report-claims

19 Corporate Europe Observatory, "There are now more Big Tech lobbyists than MEPs," November 2025, Available at: https://corporateeurope.org/en/2025/11/there-are-now-more-big-tech-lobbyists-meps

20 European Commission, *Digital Omnibus Regulation Proposal*. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

21 Corporate Europe Observatory and LobbyControl, *Article by article, how Big Tech shaped the EU's roll-back of digital rights*, January 2026. https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights. The analysis compares Commission proposal text with lobbying submissions to the EU Transparency Register from Google, Microsoft, Meta, DigitalEurope, CCIA, and ITI.

22 Corporate Europe Observatory and LobbyControl, ibid. Meta's meetings with MEPs from groups beyond the traditional centre rose from one in the previous parliamentary mandate to 38 in the current mandate, with the Digital Omnibus cited as a priority topic in those engagements.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

23 Henna Virkkunen, Executive Vice-President of the European Commission, interview with The Times, published 26 March 2026. Available at: https://www.thetimes.com/world/europe/article/eu-security-risk-us-technology-data-wz08lwpqd

24 Ibid. The technological sovereignty package is described as drawing on the European Competitiveness Fund (€234 billion over seven years) and is expected to be formally presented in May 2026. Details on the AI gigafactories component and sovereign cloud liability provisions are sourced from the same interview.

25 Capgemini, "Four of a kind: Capgemini's partnership recognized with four AWS Partner of the Year 2024 Awards," February 2025, Available at: https://www.capgemini.com/insights/expert-perspectives/four-of-a-kind-capgeminis-partnership-recognized-with-four-aws-partner-of-the-year-2024-awards/ ;

26 Capgemini, "Full-year 2025 results," press release, February 2026, Available at: https://www.capgemini.com/us-en/news/press-releases/full-year-2025-results/

27 Atos, "Multi-cloud and sovereign cloud," atos.net, Available at: https://atos.net/en/services/multi-cloud-and-sovereign-cloud

28 Devoteam Group, "2023 Financial Results," press release, 4 March 2024. Available at: https://www.devoteam.com/news-and-pr/2023-financial-results/

29 Devoteam, "Devoteam announces strategic partnership with Google Cloud to drive 2 billion USD revenue for its Google Cloud Business Unit through AI-driven transformation," press release, 23 January 2025. Available at: https://www.devoteam.com/news-and-pr/devoteam-announces-strategic-partnership-with-google-cloud/

30 CIO Dive, "CIOs face mounting pressure as IT project failure rates remain high," 14 March 2025. Available at: https://www.ciodive.com/news/cio-project-failure-career-risk-2025/

31 Nash Squared, "Digital Leadership Report 2025," annual survey of approximately 2,000 CIOs and technology leaders across Europe and North America. Directly relevant on tenure pressure, risk aversion, and decision-making constraints. Available at: https://www.nashsquared.com/dlr-2025/dlr-2025

32 Direction interministérielle du numérique (DINUM), Socle Interministériel de Logiciels Libres, maintained since 2013, 530 tools referenced as of 2025. Available at: https://sill.code.gouv.fr/

33 European Commission, Open Source Observatory (OSOR), Interoperable Europe Portal, EU OSS Catalogue (FOSSEPS initiative), 640+ solutions across 30+ public sector domains. Available at: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor

34 German Federal Ministry of the Interior, Open CoDE platform, joint repository of open-source software for German public administration. Available at: https://opencode.de

35 EU Institute for Security Studies (EUISS), "Technical is political: When a cloud certification scheme divides Europe," 3 November 2025. Available at: https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe

36 Euractiv, "Quartet of EU countries to cooperate on building sovereign digital infrastructure" 15 December 2025. Available at: https://www.euractiv.com/news/quartet-of-eu-countries-to-cooperate-on-building-sovereign-digital-infrastructure/

37 Canonical Ltd., "La Gendarmerie Nationale upgrades 85,000 PCs to Ubuntu Desktop Edition," case study, 2010. Available at: https://canonical.com/blog/la-gendarmerie-nationale-upgrades-85000-pcs-to-ubuntu-desktop-edition

38 Major Stéphane Dumond, French Gendarmerie Nationale, presentation at LibreCon 2014, Bilbao, December 2014. Available at: https://www.slideshare.net/slideshow/french-gendarmerie-nationaleubuntulibrecon2014bilbao/43013966

39 Kyndryl, press release, "Kyndryl Announces Agreement to Purchase Cloud-Services Provider Solvinity," 5 November 2025. Available at: https://www.kyndryl.com/us/en/about-us/news/2025/11/kyndryl-purchase-cloud-services-solvinity

40 NL Times, "Cabinet raises concerns over U.S. firm Kyndryl buying Solvinity, key to DigiD," 21 November 2025. Available at: https://nltimes.nl/2025/11/21/cabinet-raises-concerns-us-firm-kyndryl-buying-solvinity-key-digid ; IOPlus, "Kyndryl acquires Solvinity, raising data sovereignty concerns," 8 November 2025. Available at: https://ioplus.nl/en/posts/kyndryl-acquires-solvinity-raising-data-sovereignty-concerns-

41 Techzine Global, "Regulator investigates Kyndryl's acquisition of Dutch Solvinity," 22 January 2026. Available at: https://www.techzine.eu/news/privacy-compliance/138159/regulator-investigates-kyndryls-acquisition-of-dutch-solvinity/

42 Finnish Ministry of Justice announcement, 25 March 2026. Finnish Security and Intelligence Service (SUPO). Available at: https://supo.fi/en/cloud-adoption-obscures-the-digital-independence-of-states

43 The Register, "Europe gets serious about cutting US digital umbilical cord," 22 December 2025. Available at: https://www.theregister.com/2025/12/22/europe_gets_serious_about_cutting/

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

44 CMS Law, "White Paper: Demystifying the Debate on the US CLOUD Act vs. European/UK Data Sovereignty in the Context of Cloud Services," *CMS LawNow*, February 2026. Available at: https://cms-lawnow.com/en/ealerts/2026/02/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data-sovereignty-in-the-context-of-cloud-services. The white paper notes that in the absence of a US-EU executive agreement, cloud providers lack a formal legal mechanism to invoke conflict-of-law review against American production orders.

45 S3NS / BusinessWire, "S3NS Announces SecNumCloud Qualification for PREMI3NS, its Trusted Cloud Offering," 19 December 2025. Available at: https://www.businesswire.com/news/home/20251218817208/en/S3NS-Announces-SecNumCloud-Qualification-for-PREMI3NS-its-Trusted-Cloud-Offering; LeMagIT, "S3NS annonce l'obtention de la qualification SecNumCloud," 19 December 2025. Available at: https://www.lemagit.fr/actualites/366636681/S3NS-annonce-lobtention-de-sa-qualification-SecNumCloud

46 Bleu, press release, "Bleu franchit une étape importante vers le cloud de confiance: l'ANSSI valide le jalon J0," 17 April 2025. Available at: https://www.bleucloud.fr/bleu-valide-le-j0-de-la-qualification-secnumcloud-3-2/ ; Usine Digitale, "Cloud de confiance: Bleu passe le jalon J1 pour la qualification SecNumCloud 3.2," 18 November 2025. Available at: https://www.usine-digitale.fr/article/cloud-de-confiance-bleu-passe-le-jalon-j1-pour-la-qualification-secnumcloud-3-2.N2241512

47 Conseil d'État, decision of 20 March 2026, rejecting recourses against CNIL deliberation n° 2025-013 of 13 February 2025 authorising the EMC2 project (Health Data Hub hosting on Microsoft Azure). Reported in: La Tribune, *Le Conseil d'Etat valide l'hébergement par Microsoft des données de santé de 10 millions de Français* , 20 March 2026, https://www.latribune.fr/article/tech/84041921343671/le-conseil-detat-valide-lhebergement-par-microsoft-des-donnees-de-sante-de-10-millions-de-francais. For the CNIL's own characterisation of the residual risk, see also: Next.ink, *La CNIL autorise les données de santé chez Microsoft*, February 2024, https://www.conseil-etat.fr/actualites/health-data-hub-le-traitement-automatise-des-donnees-de-sante-autorise-par-la-cnil-est-conforme-au-rgpd

48 Senate inquiry testimony of 28 May 2025. Available at: https://www.senat.fr/compte-rendu-commissions/20250526/ce_comm_pub.html#toc5

49 The Register, "Microsoft's data sovereignty: Now with extra sovereignty!", 7 November 2025. Available at: https://www.theregister.com/2025/11/07/microsoft_announces_strengthening_of_sovereignty/

50 Roland Busch, chief executive of Siemens, interview with the Financial Times, 25 March 2026. Available at: https://www.ft.com/content/d66e857d-803b-45b8-b2f4-3c433b79bfc5?syn-25a6b1a6=1

51 Synergy Research Group, Q2 2024, cited in IT Pro, "Sovereign infrastructure spend to triple in Europe," February 2026. Available at: https://www.itpro.com/infrastructure/sovereign-infrastructure-spend-to-triple-in-europe-as-fifth-of-workloads-stay-local. EUISS, "Technical is political," November 2025 (op. cit.)

52 Scaleway, "Custom-built Clusters," Available at: https://www.scaleway.com/en/custom-built-clusters/ (Arthur Mensch quote, ai-PULSE 2023) ; Data Center Dynamics, "Mistral AI raises €1.7bn in funding round led by ASML," February 2026, Available at: https://www.datacenterdynamics.com/en/news/mistral-ai-raises-17bn-in-funding-round-led-by-asml/ (40MW Essonne cluster hosted by Scaleway, announced February 2026)

53 Daskal, Jennifer, "Unpacking the CLOUD Act," *EUCRIM: The European Criminal Law Review*, No. 2 (2019), pp. 123-129. Daskal identifies the Act as "a much-needed attempt" to clarify extraterritorial obligations while acknowledging unresolved conflicts with European law. Available at: https://eucrim.eu/media/articles/pdf/eucrim-article-2018-022.pdf

54 Congressional Research Service (CRS), *Cross-Border Data Sharing Under the CLOUD Act*, Report R45173, April 2018, updated 2019. Available at: https://crsreports.congress.gov/product/pdf/R/R45173

55 As of March 2026, no EU-US bilateral executive agreement under the CLOUD Act has entered into force, meaning the Act's conflict-of-law review mechanism does not apply to requests involving European Union member states.

56 Speed, Richard, "Canadian data order risks blowing a hole in EU sovereignty," *The Register*, 27 November 2025. Available at: https://www.theregister.com/2025/11/27/canada_court_ovh/

57 Ibid. The ruling by Justice Heather Perkins-McVey, Ontario Court of Justice, dated 25 September 2025, stated: *"The Court must balance the interests of the state and the respondent"* and found in favour of the production order on national security grounds. See also: Heise Online, "Canadian Court: OVHcloud from France must hand over user data," 27 November 2025. https://www.heise.de/en/news/Canadian-Court-OVHcloud-from-France-must-hand-over-user-data-11092029.html

58 Gartner, press release, "Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026," 9 February 2026. Available at: https://www.gartner.com/en/newsroom/press-releases/2026-02-09-gartner-says-worldwide-sovereign-cloud-iaas-spending-will-total-us-dollars-80-billion-in-2026

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

59 MarketsandMarkets, *Identity and Access Management (IAM) Market by Technology, Type, Identity Type, Deployment Mode, Vertical - Global Forecast to 2030*, Report TC 3138, November 2025. Available at: https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html

60 Ibid. The report's competitive landscape section identifies Microsoft, Ping Identity, and IBM as "Star players" delivering "comprehensive end-to-end identity solutions" with "strong global presence," and lists no European vendor in any competitive category.

61 SAM Expert, "Microsoft Entra ID Faces Global Antitrust Probes," 26 September 2025. Available at: https://samexpert.com/entra-id-antitrust-probes/

62 ProPublica, "Microsoft Is the Target of a Wide-Ranging FTC Antitrust Investigation," 27 November 2024. Available at: https://www.propublica.org/article/ftc-investigating-microsoft-antitrust-cloud-computing; Fortune, "Microsoft faces broad antitrust investigation from U.S. FTC," 27 November 2024. Available at: https://fortune.com/2024/11/27/microsoft-antitrust-investigation-ftc/ ; SAMexpert, "FTC vs Microsoft: The Broadest Antitrust Probe Since the 1990s," September 2025. Available at: https://samexpert.com/ftc-microsoft-investigation-2025/

63 Inteca, "2025 Keycloak Pricing: Understanding the Cost of Managed Service," 20 May 2025. Available at: https://inteca.com/business-insights/keycloak-pricing-guide-2025-cost-estimation-for-hosting-open-source-identity-and-access-management/

64 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183

65 MSSP Alert, "Gartner Magic Quadrant Names Microsoft, SentinelOne Among EPP Leaders," 2 October 2024. Available at: https://www.msspalert.com/feature/gartner-magic-quadrant-names-microsoft-sentinelone-among-epp-leaders/

66 Mordor Intelligence, "Endpoint Security Market Report 2025-2030," February 2026 (Lenovo/SentinelOne factory default). Available at: https://www.mordorintelligence.com/industry-reports/global-endpoint-security-market-industry

67 TechTarget, "CrowdStrike outage explained: What caused it and what's next," updated 2024. Available at: https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next ; Messageware, "What Caused the CrowdStrike Outage: A Detailed Breakdown." Available at: https://www.messageware.com/what-caused-the-crowdstrike-outage-a-detailed-breakdown/

68 Privacy International, "CrowdStrike: What the 2024 outage reveals about security." Available at: https://privacyinternational.org/long-read/5507/crowdstrike-what-2024-outage-reveals-about-security ; SecurityWeek, "Microsoft's Take on Kernel Access and Safe Deployment Following CrowdStrike Incident," October 2024. Available at: https://www.securityweek.com/microsofts-take-on-kernel-access-and-safe-deployment-practices-following-crowdstrike-incident/

69 HarfangLab, "HarfangLab, premier EDR à recevoir une qualification de l'ANSSI," January 2025. Available at: https://harfanglab.io/fr/press/harfanglab-premier-edr-a-recevoir-une-qualification-de-lanssi/ ; HarfangLab, "MITRE 2024: HarfangLab reaffirms its European leader position," December 2024. Available at: https://harfanglab.io/press/tests-mitre-2024-ledr-dharfanglab-confirme-sa-position-de-leader-europeen/ ; Techzine Global, "HarfangLab positions itself as the open and European EDR player," January 2025. Available at: https://www.techzine.eu/blogs/security/127790/harfanglab-positions-itself-as-the-open-and-european-edr-player/

70 HarfangLab, "HarfangLab's EDR is the first to receive BSI Certification." Available at: https://ecs-org.eu/harfanglabs-edr-is-the-first-to-receive-bsi-certification/

71 Sekoia.io, product page. Available at: https://www.sekoia.io/en/homepage/

72 AV-TEST, "Advanced EDR test 2024: WithSecure Elements Endpoint Detection and Response." Available at: https://www.av-test.org/en/news/advanced-edr-test-2024-withsecure-elements-endpoint-detection-and-response/

73 Apple Developer, WWDC 2019 session "System Extensions and DriverKit" (announced deprecation); Apple Developer, WWDC 2020 session "Build an Endpoint Security app," Available at: https://developer.apple.com/videos/play/wwdc2020/10159/; Trail of Bits, "Sinter: New user-mode security enforcement for macOS," 12 August 2020, Available at: https://blog.trailofbits.com/2020/08/12/sinter-new-user-mode-security-enforcement-for-macos/

74 Open Cloud Coalition, cited in Digital Samba, "Europe's Dependency on Microsoft: A Threat to Its Digital Sovereignty?", August 2025. Available at: https://www.digitalsamba.com/blog/europes-dependency-on-microsoft-a-threat-to-its-digital-sovereignty ;

75 Computerworld, "Gov't IT spending seen as key to building Europe's tech ecosystem," 6 March 2026. Available at: https://www.computerworld.com/article/4141925/govt-it-spending-seen-as-key-to-building-europes-tech-

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ecosystem.html (direct quote from Rebecca Lenhard, MdB, Green Party, Bundestag Committee on Digital Transformation and Government Modernization, speaking at a Nextcloud roundtable, March 2026)

76 Asteres, "La dépendance technologique aux softwares & cloud services américains: une estimation des conséquences économiques en Europe", April 2025. Available at: https://asteres.fr/etude/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe/

77 Nextcloud, "About Nextcloud," Available at: https://nextcloud.com/about/

78 Nextcloud, press release, "Austrian Federal Ministry for Economic Affairs deploys Nextcloud," October 2025, Available at: https://nextcloud.com/blog/pres/

79 Siècle Digital, "Suite Numérique: l'État accélère sa révolution tech," 1 December 2025. Available at: https://siecledigital.fr/2025/12/01/suite-numerique-letat-accelere-sa-revolution-tech-avec-une-alternative-souveraine-aux-geants-americains/

80 Henna Virkkunen, Executive Vice-President of the European Commission, and French government commitment cited in: The Times, *Europeans should use homegrown alternatives to American software*, 26 March 2026. Available at: www.thetimes.com/world/europe/article/eu-security-risk-us-technology-data-wz08lwpqd
The French commitment is described as an order to ministries to migrate from Zoom and Microsoft Teams to Visio hosted on French national infrastructure, with a 2027 completion target.

81 Figures vary by source. The Cour des Comptes reported 190,000 Tchap users as of mid-2024. Framasoft (March 2026) cites approximately 300,000 monthly active accounts against 600,000 total registered accounts. A figure of 375,000 monthly active users circulates in trade press without primary source attribution. The directional trend is consistent across all sources.

82 Usine Digitale, "La Suite Numérique: l'État ambitionne de bâtir une alternative souveraine crédible," 28 November 2025. Available at: https://www.usine-digitale.fr/souverainete/la-suite-numerique-letat-ambitionne-de-batir-une-alternative-souveraine-credible-face-aux-grandes-suites-bureautiques-americaines.EAX2IPKLWRDRVL25FKZUJV3U2E.html

83 Cour des comptes, "Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique," 10 July 2024. Available at: https://www.ccomptes.fr/fr/publications/le-pilotage-de-la-transformation-numerique-de-letat-par-la-direction ; summary Available at: https://solutions-entreprise.developpez.com/actu/360577/France-la-strategie-numerique-de-l-Etat-mise-en-oeuvre-par-la-DINUM-est-illisible/

84 Next, "L'Éducation nationale signe pour au moins 74 millions d'euros de solutions et services Microsoft," 18 March 2025. Available at: https://next.ink/175788/leducation-nationale-signe-pour-100-millions-deuros-de-solutions-et-services-microsoft/ ; contract attribution notice published 14 March 2025, Lots 1 and 2 awarded to Crayon France. See also: CIO Online, "Licences Microsoft: l'Éducation Nationale joue au mauvais élève," Available at: https://www.cio-online.com/actualites/lire-licences-microsoft-l-education-nationale-joue-au-mauvais-eleve-16235.html

85 Assemblée nationale, Question écrite n°5312, Philippe Latombe (Les Démocrates, Vendée). Available at: https://www.assemblee-nationale.fr/dyn/17/questions/QANR5L17QE5312

86 Hexatrust, "L'éducation nationale hébergée chez Microsoft: la souveraineté numérique en échec scolaire ?", 21 March 2025. Available at: https://www.hexatrust.com/leducation-nationale-hebergee-chez-microsoft-la-souverainete-numerique-en-echec-scolaire/

87 Next, "Vent de fronde contre le choix de Microsoft par l'Éducation nationale et l'École Polytechnique." Available at: https://next.ink/176974/vent-de-fronde-contre-le-choix-de-microsoft-par-leducation-nationale-et-lecole-polytechnique/

88 SBS Software, "Why Wero is Europe's best bet to compete in the global payment race," October 2025. Available at: https://sbs-software.com/insights/wero-europe-payment-race/

89 Instant Payment Regulation (EU) 2024/886, entered into force April 2024; PayRam, "European Payments Initiative Wero: EPI vs Visa Mastercard," February 2026. Available at: https://payram.com/blog/european-payments-initiative-wero

90 EPI, interview presented by the European Payment Council. *Wero: Shaping the future of European payments*. Available at: https://www.europeanpaymentscouncil.eu/news-insights/insight/wero-shaping-future-european-payments

91 EPI, *PSA prepares issuing support for Wero in Austria and Germany*. Available at: https://epicompany.eu/media-insights/psa-prepares-issuing-support-for-wero-in-austria-and-germany

92 European Business Magazine, "Europe's $24 Trillion Breakup With Visa and Mastercard Has Begun," February 2026. Available at: https://europeanbusinessmagazine.com/business/europes-24-trillion-breakup-with-visa-and-mastercard-has-begun/

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

93 Philippdubach.com, "Europe's €24 Trillion Payment Breakup," February 2026. Available at: https://philippdubach.com/posts/europes-24-trillion-payment-breakup-is-really-a-bet-on-infrastructure-arbitrage/

94 "How close is the EU to break free from Visa and Mastercard's grip?", 3 March 2026. Available at: https://www.euronews.com/my-europe/2026/03/03/how-close-is-the-eu-to-break-free-from-visa-and-mastercards-grip

95 Council Regulation (EC) No 2271/96 of 22 November 1996, as amended by Commission Delegated Regulation (EU) 2018/1100. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31996R2271

96 Field fisher, "International firms caught between US Iran sanctions and EU blocking statute", 2018. Available at: https://www.fieldfisher.com/en/insights/international-firms-caught-between-us-iran-sanctions-and-eu-blocking-statute

97 Andreas Floemer, *Paying without Google: New consortium wants to remove custom ROM hurdles*, heise online, 9 March 2026. https://www.heise.de/en/news/Paying-without-Google-New-consortium-wants-to-remove-custom-ROM-hurdles-11204037.html

98 Cloudflare, *DDoS Threat Report Q4 2025*, January 2026. Available at: https://blog.cloudflare.com/ddos-threat-report-2025-q4/

99 MarketsandMarkets, *DDoS Protection and Mitigation Security Market by Solution Type — Global Forecast to 2030*, Report TC 4985, November 2025. Available at: https://www.marketsandmarkets.com/Market-Reports/ddos-protection-mitigation-market-111952874.html. The report identifies the primary vendors as NetScout, Akamai, Radware, Fortinet, Cloudflare, and Microsoft; no European operator appears in the competitive landscape.

100 Cloudflare, post-mortem blog post, "Cloudflare outage on December 5, 2025," 10 December 2025. Available at: https://blog.cloudflare.com/5-december-2025-outage/ (primary source, authored by Cloudflare engineering team); Cisco ThousandEyes, "Cloudflare Outage Analysis: December 5, 2025," Available at: https://www.thousandeyes.com/blog/cloudflare-outage-analysis-december-5-2025 (independent third-party technical analysis)

101 Bunny.net, product page. Available at: https://bunny.net ; ConceptRecall, "Bunny.net: The Best Cloudflare Alternative," November 2025. Available at: https://conceptrecall.com/blog/bunny-net-best-cloudflare-alternative

102 Jonathan Frere, "Switching to BunnyCDN in Less Than 2 Hours," 9 March 2025. Available at: https://jonathan-frere.com/posts/switching-to-bunny-cdn/

103 Gcore, product documentation. Available at: https://gcore.com/ddos-protection

104 Cloudflare, "Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report," October 2025. Available at: https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/

105 Previsible, "AI Traffic Is Up 527%. SEO Is Being Rewritten," *Search Engine Land*, 5 August 2025. The figure derives from analysis of 19 Google Analytics 4 properties comparing January-May 2024 with January-May 2025; total AI-referred sessions grew from 17,076 to 107,100 across the dataset. https://searchengineland.com/ai-traffic-up-seo-rewritten-459954

106 Statcounter Global Stats, *Search Engine Market Share Worldwide*, Q4 2024; reported by Danny Goodwin, "Google's Search Market Share Drops Below 90% for First Time Since 2015," *Search Engine Land*, 2 January 2025. Google's global share recorded 89.34% in October, 89.99% in November, and 89.73% in December 2024. https://searchengineland.com/google-search-market-share-drops-2024-450497

107 Gartner, "Gartner Predicts Search Engine Volume Will Drop 25% by 2026, Due to AI Chatbots and Other Virtual Agents," press release, 19 February 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-19-gartner-predicts-search-engine-volume-will-drop-25-percent-by-2026-due-to-ai-chatbots-and-other-virtual-agents

108 Walton Family Foundation and GSV Ventures, Gen Z Is Using AI — But Reports Gaps in School and Workplace Support, Gallup Panel survey of 3,465 respondents aged 13-28, conducted 6-13 March 2025, margin of error ±2.4 percentage points. https://www.waltonfamilyfoundation.org/about-us/newsroom/gen-z-is-using-ai-but-reports-gaps-in-school-and-workplace-support

109 Richard Fletcher and Rasmus Kleis Nielsen, *Generative AI and News Report 2025*, Reuters Institute for the Study of Journalism, Oxford, 2025: weekly use of generative AI across six countries nearly doubled from 18% in 2024 to 34% in 2025. https://reutersinstitute.politics.ox.ac.uk/generative-ai-and-news-report-2025-how-people-think-about-ais-role-journalism-and-society

110 Commission Nationale de l'Informatique et des Libertés (CNIL), formal notice of 10 February 2022 finding that transfers of personal data to the United States via Google Analytics violate Article 44 et seq. of the GDPR, issued in coordination with European counterpart authorities following complaints by noyb. https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure

111 European Commission, Commission Implementing Decision designating Alphabet Inc. as gatekeeper pursuant to Article 3(4) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

markets in the digital sector, 6 September 2023. Google Search and Google's advertising services are among the eight core platform services designated for Alphabet. Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng . Press release at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

112 OECD, "AI firms capture 61% of global venture capital in 2025," press release, February 2026. Available at: https://www.oecd.org/en/about/news/announcements/2026/02/ai-firms-capture-61-percent-of-global-venture-capital-in-2025.html. Full report: OECD, "Venture capital investments in artificial intelligence through 2025." Available at: https://www.oecd.org/en/publications/venture-capital-investments-in-artificial-intelligence-through-2025_a13752f5-en/full-report.html

113 Stanford University HAI, AI Index Report 2025, Chapter: Economy. Available at: https://hai.stanford.edu/ai-index/2025-ai-index-report/economy. 2024 figures: U.S. private AI investment $109.1 billion (81% of global total), China $9.3 billion, UK $4.5 billion. U.S.-based institutions produced 40 notable AI models in 2024 against 3 from the EU27.

114 Mistral AI, "Introducing Mistral 3," December 2025. Available at: https://mistral.ai/news/mistral-3. ASML, press release, "ASML invests in Mistral AI as lead investor in Series C," 9 September 2025; confirmed by Reuters, CNBC, and Euronews on the same date. ASML's investment of approximately €1.3 billion corresponds to an equity stake of approximately 11%. European AI & Cloud Summit, "Mistral AI's $14 billion valuation marks Europe's AI turning point," 2025. Available at: https://cloudsummit.eu/blog/mistral-ai-14-billion-valuation-europe-turning-point

115 Generation Digital, "Mistral AI wins French defence AI framework agreement," January 2026. Available at: https://www.gend.co/blog/mistral-ai-french-defence-framework ; Mistral AI, Government solutions page. Available at: https://mistral.ai/solutions/ai-for-citizens

116 European AI & Cloud Summit (op. cit.); InfoWorld, "Mistral AI deepens compute ambitions with Koyeb acquisition," February 2026. Available at: https://www.infoworld.com/article/4133757/mistral-ai-deepens-compute-ambitions-with-koyeb-acquisition.html

117 NVIDIA Newsroom, "Europe Builds AI Infrastructure With NVIDIA to Fuel Region's Next Industrial Transformation," 11 June 2025. Available at: https://nvidianews.nvidia.com/news/europe-ai-infrastructure

118 CNBC, "Mistral AI announces billion-dollar AI infrastructure push in Sweden," 11 February 2026. Available at: https://www.cnbc.com/2026/02/11/mistral-ai-infrastructure-sweden.html

119 Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 (European Chips Act), Article 1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1781 ; European Commission, "European Chips Act," digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-chips-act ; Science|Business, "EU governments set out priorities for Chips Act 2.0," 29 September 2025. Available at: https://sciencebusiness.net/news/semiconductors/eu-governments-set-out-priorities-chips-act-20

120 European AI & Cloud Summit (op. cit.); InfoWorld, "Mistral AI deepens compute ambitions with Koyeb acquisition," February 2026. Available at: https://www.infoworld.com/article/4133757/mistral-ai-deepens-compute-ambitions-with-koyeb-acquisition.html

121 European Commission, "AI Factories," digital-strategy.ec.europa.eu, updated 2026. Available at: https://digital-strategy.ec.europa.eu/en/policies/ai-factories. The InvestAI facility comprises a €20 billion fund to create up to five AI Gigafactories, each integrating over 100,000 advanced AI processors. For operational details on the procurement timeline: Light Reading, "EU defers formal call for AI gigafactories to early 2026," 4 December 2025. Available at: https://www.lightreading.com/ai-machine-learning/eu-defers-formal-call-for-ai-gigafactories-to-early-2026

122 Aleph Alpha, customer references, Available at: https://aleph-alpha.com

123 AMD, press release, "AMD Completes Acquisition of Silo AI to Accelerate Development and Deployment of AI Models on AMD Hardware," 10 July 2024. Available at: https://www.amd.com/en/newsroom/press-releases/2024-8-12-amd-completes-acquisition-of-silo-ai-to-accelerate.html

124 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

125 GitHub Blog, "npm is joining GitHub," 16 March 2020. Available at: https://github.blog/news-insights/company-news/npm-is-joining-github/ (announcement by GitHub CEO Nat Friedman); GitHub Blog, "npm has joined GitHub," 15 April 2020. Available at: https://github.blog/news-insights/company-news/npm-has-joined-github/ (completion confirmation)

126 Electroiq, "GitHub Statistics And Facts, By Users, Security And Repos," September 2025. Available at: https://electroiq.com/stats/github-statistics/

127 GitHub, "Racing into 2025 with new GitHub Innovation Graph data," GitHub Blog, 21 April 2025, https://github.blog/news-insights/research/racing-into-2025-with-new-github-innovation-graph-data/. Dataset

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

available at https://innovationgraph.github.com. For independent validation, see: Korkmaz, G. et al., "From GitHub to GDP: A framework for measuring open source software innovation," *Research Policy*, Vol. 53, No. 3 (2024), https://doi.org/10.1016/j.respol.2024.104954.

128 GitHub, press release, "GitHub Offers Data Residency in the EU with GitHub Enterprise Cloud," 24 September 2024. Available at: https://github.com/newsroom/press-releases/data-residency-in-the-eu

129 RedMonk, "Is npm Enough? Why Startups are Coming after this JavaScript Package Registry," 30 January 2025. Available at: https://redmonk.com/kholterhoff/2025/01/30/is-npm-enough/

130 Open CoDE platform, Available at: https://opencode.de

131 Forgejo, "Forgejo forks its own path forward," February 2024. Available at: https://forgejo.org/2024-02-forking-forward/ ; Forgejo, "Forgejo is now licensed under the GPL," August 2024. Available at: https://forgejo.org/2024-08-gpl/ ; Forgejo, "Comparison with Gitea." Available at: https://forgejo.org/compare-to-gitea/

132 owu.se, "Gitea and Forgejo, Late 2024 Edition," January 2025. Available at: https://owu.se/blog/gitea-and-forgejo

133 LinuxSecurity, "Supply Chain Attacks Impact NPM, PyPI, and Docker Hub," 27 November 2025. Available at: https://linuxsecurity.com/features/supply-chain-attacks-npm-pypi-docker

134 Direction Interministérielle du Numérique (DINUM), code.gouv.fr. Available at: https://code.gouv.fr

135 GitHub, *GitHub Copilot Privacy Statement*, updated October 2024. The statement confirms that code context (including surrounding code, file content, and repository metadata) is transmitted to GitHub's servers to generate completions. For Enterprise and Business plans with telemetry disabled, prompts are not retained for model training; for individual accounts without explicit opt-out, transmission remains. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy

136 U.S. Department of Commerce, Bureau of Industry and Security, *Addition of Huawei Technologies Co., Ltd. to the Entity List*, Federal Register, 21 May 2019. Entity List designation under Export Administration Regulations, prohibiting U.S. companies from supplying Huawei without a licence. https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-huawei-technologies-co-ltd-to-the-entity-list

137 Reuters, *Google suspends some business with Huawei after Trump blacklist*, 19 May 2019. Android licence suspension effective immediately; Huawei to lose access to Play Store, Gmail, and Android security updates for new devices. Temporary General Licence issued 20 May 2019 granting 90-day reprieve for existing devices only. Reported by multiple outlets including NPR, XDA Developers, and Android Authority. https://www.reuters.com/article/world/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-sou-idUSKCN1SP0N7/

138 *Bloomberg, Qualcomm, Intel, Broadcom and ARM Cut Off Huawei*, 20 May 2019. Multiple U.S. semiconductor suppliers suspended shipments to Huawei within days of Entity List designation. https://www.gadgetmatch.com/intel-broadcom-qualcomm-huawei-us-ban/

139 NPR, *U.S. Delays Ban; Huawei Phones Will Get Android Updates*, 20 May 2019. Reference to Huawei CEO Ren Zhengfei's prior acknowledgement of the risk and development of contingency operating system. https://www.npr.org/2019/05/20/724910121/after-trump-ban-huawei-phones-will-lose-access-to-google-software

140 European Union Agency for Cybersecurity (ENISA), *Subsea Cables - What Is at Stake?*, July 2023, ISBN 978-92-9204-612-5, DOI 10.2824/212261. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20at%20stake%20report.pdf

141 AmCham EU, BSA, CCIA Europe, ITI, *Joint industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements*, 2023. Full text and signatories: https://www.uschamber.com/security/cybersecurity/joint-industry-statement-on-the-need-for-a-swift-adoption-of-the-eu-cybersecurity-certification-scheme-for-cloud-services-without-sovereignty-requirements. https://ccianet.org/wp-content/uploads/2023/05/Joint-Industry-Statement-on-EUCS.pdf https://www.amchameu.eu/position-papers/joint-industry-statement-need-swift-adoption-eu-cybersecurity-certification-scheme https://www.ebf.eu/ebf-media-centre/joint-industry-statement-calls-for-removing-sovereignty-requirements-from-european-cybersecurity-certification-scheme-for-cloud-services-eucs/The statement was subsequently shared with the U.S. Secretary of State, Trade Representative, and Secretary of Commerce in advance of the EU-U.S. Trade and Technology Council meeting.

142 ITI, *ITI urges EU lawmakers to drop sovereignty requirements in final EUCS*, April 2024, https://www.itic.org/news-events/news-releases/iti-urges-eu-lawmakers-to-drop-sovereignty-requirements-in-final-eucs. ITI explicitly commended the March 2024 draft for removing sovereignty requirements, describing them as "politically motivated" and "discriminatory." Full submission: https://www.itic.org/documents/europe/20240411ITIrecommendationsonthefinalizationoftheEUCS.pdf

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

143 Hogan Lovells, *EUCS: Controversial sovereignty issues continue to drive debate for cloud services*, June 2024, https://www.hoganlovells.com/en/publications/eucs-controversial-data-sovereignty-issues-continue-to-drive-debate-around-the-eu-certification-scheme-for-cloud-services. For the broader geopolitical context of the removal: EU Institute for Security Studies, *Technical is political: when a cloud certification scheme divides Europe*, November 2025, https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe

144 European Commission, EUCS relaunch communications, January 2026. The Cloud Access for Data Act (CADA) is described in Commission communications as the instrument designed to address data access and sovereignty questions outside the technical certification scope of the EUCS. Status and binding force of the CADA were not fully determined at the time of publication of this report. Progress to monitor via ENISA consultation calendar and the European Parliament ITRE committee.

145 BWI GmbH / Bundeswehr, *BwMessenger - Sichere Kommunikation der Deutschen Bundeswehr auf dem Open Source Protokoll Matrix*, OSS Directory case study. BwMessenger launched November 2020, now used daily by more than 100,000 Bundeswehr personnel. Source code published on Open CoDE. Available at: https://www.ossdirectory.com/en/success-stories/details/bwmessenger-sichere-kommunikation-der-deutschen-bundeswehr-auf-dem-open-source-protokoll-matrix

146 Interoperable Europe Portal, *BundesMessenger: Shared, Reused and Interoperable*, 16 June 2023: BundesMessenger, derived from BwMessenger, released December 2023 for use by all German public authorities; explicitly designed for federation with Tchap, noting that cross-instance communication between French and German government Matrix deployments is achievable without additional integration work. Available at: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/bundesmessenger-shared-reused-and-interoperable

147 Anu Bradford, *The Brussels Effect: How the European Union Rules the World*

148 Mlex, Olivier Guersent: “We're so *grossly understaffed* that we have to make priorities choices that are difficultly compatible with the policy objectives we're pursuing”. Available at: https://www.mlex.com/mlex/articles/2322385/

149 Schleswig-Holstein Digitalisierungsministerium, statement by Minister Dirk Schrödter, December 2025. Reported in: heise online, *Goodbye, Microsoft: Schleswig-Holstein relies on Open Source and saves millions*, 7 December 2025, available at https://www.heise.de/en/news/Goodbye-Microsoft-Schleswig-Holstein-relies-on-Open-Source-and-saves-millions-11105459.html

150 Silicon.fr, *Le Health Data Hub vers un hébergement SecNumCloud*, 9 February 2026, Available at https://www.silicon.fr/cloud-1370/le-health-data-hub-vers-un-hebergement-secnumcloud-225631

151 French government statement confirming American hyperscalers excluded from UGAP Nuage Public procurement for Health Data Hub successor. Reported in: L'Usine Digitale, *Health Data Hub, EMC2: les données de santé des Français prisonnières de Microsoft?*, https://www.usine-digitale.fr/article/health-data-hub-emc2-les-donnees-de-sante-des-francais-prisonnieres-de-microsoft.N2224051. On the contested characterisation of eligibility criteria: at least one market participant disputed whether SecNumCloud appeared as an eligibility condition or a scoring factor;

152 the Ministry of Health declined to transmit the criteria text. Reported in: L'Usine Digitale, ibid.

153 OpenStudio, "L'Open Source au sein d'une collectivité territoriale — Nicolas Vivant", 21 octobre 2025, https://www.openstudio.fr/2025/10/21/lopen-source-au-sein-dune-collectivite-territoriale-nicolas-vivant/

154 LinuxFr.org, "Économies réalisées grâce aux logiciels libres sur la commune d'Échirolles: 2M d'euros sur un mandat", 16 mai 2024, https://linuxfr.org/users/dzecniv/liens/economies-realisees-grace-aux-logiciels-libres-sur-la-commune-d-echirolles-2m-d-euros-sur-un-mandat

155 L'Âge de Faire, "Vers des collectivités libres", 7 novembre 2025, https://lagedefaire-lejournal.fr/vers-des-collectivites-libres/

156 Libre à lire, "Passer au libre, c'est changer de monde", conférence France Numérique Libre 2025, 15 novembre 2025, https://www.librealire.org/passer-au-libre-c-est-changer-de-monde

157 Smart City Mag, "Comment la Ville d'Échirolles pousse au maximum l'utilisation de logiciels libres", 4 décembre 2024, https://www.smartcitymag.fr/article/1542/comment-la-ville-d-echirolles-pousse-au-maximum-l-utilisation-de-logiciels-libres

158 Next.ink, "Municipales: 'passer aux logiciels libres, c'est faisable, on l'a fait', mais…", 2026, https://next.ink/226555/municipales-passer-aux-logiciels-libres-cest-faisable-on-la-fait-mais/

159 Frandroid, “Les impôts français (DGFIP) pourraient bien abandonner Windows”. Available at: https://www.frandroid.com/marques/microsoft/3004473_les-impots-francais-dgfip-pourraient-bien-abandonner-windows

160 GendBuntu project timeline and technical documentation: Wikipedia, *GendBuntu*, last updated August 2025, sourced from IDABC/OSOR case study (European Commission Joint Research Centre), Canonical case study

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

(2010), and presentation by Major Stéphane Dumond, LibreCon 2014, Bilbao. Cumulative savings figure of €50 million and 40% TCO reduction: cited in OSOR case study and corroborated by multiple secondary sources. Annual saving of €2 million: primary source, Commandant Jean-Pascal Chateau, Canonical case study, 2010, available at https://canonical.com/blog/la-gendarmerie-nationale-upgrades-85000-pcs-to-ubuntu-desktop-edition

161 heise online, *Goodbye, Microsoft: Schleswig-Holstein relies on Open Source and saves millions*, 7 December 2025. Annual licence savings exceeding €15 million from 2026; one-time transition costs of €9 million. Available at: https://www.heise.de/en/news/Goodbye-Microsoft-Schleswig-Holstein-relies-on-Open-Source-and-saves-millions-11105459.html

162 IT's FOSS News, *Schleswig-Holstein Completes Massive Migration to Open Source Email Systems*, 10 October 2025. Migration of 40,000 mailboxes and 100 million emails and calendar entries from Microsoft Exchange and Outlook to Open-Xchange and Thunderbird, completed 2 October 2025, covering approximately 30,000 employees. Available at: https://news.itsfoss.com/schleswig-holstein-email-system-migration/

163 Raconteur, *Meet the German local government showing Microsoft the red card*, 11 July 2025. Schrödter's framing of the migration as a structural dependency issue; quote on state responsibility to control its own IT processes and ensure data security. Available at: https://www.raconteur.net/technology/schleswig-holstein-open-source

164 eGovernment, *Open Source: beste Voraussetzungen für den Umstieg*, 18 December 2024. ODF mandate as official document format for Schleswig-Holstein state administration, effective 1 August 2024. Available at: https://www.egovernment.de/open-source-beste-voraussetzungen-fuer-den-umstieg-a-a763f0e044ccb231f11cb2d019fbf5f2/

165 Heise online, ibid. (endnote 150). Minister Schrödter's public letter acknowledging operational difficulties; opposition criticism regarding the gap between workplaces converted on paper and employees able to work with them properly.

166 Irish Times, *A small German state's quiet revolt against Microsoft*, 14 February 2026. Bipartisan commitment from CDU and Green coalition partners; migration surviving government formation. Available at: https://www.irishtimes.com/world/europe/2026/02/14/a-small-german-states-quiet-revolt-against-microsoft-and-what-it-means-for-europe/

167 Raconteur, ibid. (endnote 163). Open Source Program Office; local innovation hub; reframing of licence savings as investment in domestic digital economy; Schrödter quote on redirecting IT funding from licence fees to development and support contracts.

168 IT's FOSS News, ibid. (endnote 162). Commitment to share migration tools and experiences with other regions and institutions; documented interest from Denmark, the UK, France, New Zealand, India, Switzerland, and Austria.

169 Open Source For You, *International Criminal Court Drops Microsoft 365 For Open Source openDesk Platform*, 7 November 2025. Migration covers approximately 1,800 workstations; decision follows Karim Khan account lockout in May 2025. https://www.opensourceforu.com/2025/11/international-criminal-court-drops-microsoft-365-for-open-source-opendesk-platform/

170 EJIL Talk, *Justice Recoded? Why It Matters that the International Criminal Court Embraced Open-Source Software and Ditched Microsoft*, 10 November 2025. Confirmed date of ICC announcement (31 October 2025); September 2025 emergency meetings following threat of entity-wide sanctions; ZenDiS and EU Digital Commons EDIC context. https://www.ejiltalk.org/justice-recoded-why-it-matters-that-the-international-criminal-court-embraced-open-source-software-and-ditched-microsoft/

171 Brussels Signal, *ICC ditches Microsoft Office in favour of German state-owned software*, 31 October 2025. Direct quote from ICC Head of Digital Services. https://brusselssignal.eu/2025/10/icc-ditches-microsoft-office-in-favour-of-german-state-owned-software/

172 Cybernews, *ICC replacing Microsoft workplace software with OpenDesk*, 3 November 2025. Timeline of sanctions executive order (February 2025), Karim Khan account loss (May 2025), migration confirmation (October 2025), Brad Smith denial. https://cybernews.com/tech/icc-replacing-microsoft-workplace-software-opendesk/

173 Computing.co.uk, *ICC drops Microsoft for open source*, October 2025. Scale qualifier: "the ICC is a relatively small Microsoft customer, with under 2,000 workstations." https://www.computing.co.uk/news/2025/open-source/international-criminal-court-drops-microsoft

174 Erasmus Magazine, *International Criminal Court dumps Microsoft. Can a university of applied sciences or university do the same?*, 17 November 2025. Expert assessment on generalisability of accelerated migration under pressure. https://www.erasmusmagazine.nl/en/2025/11/17/international-criminal-court-dumps-microsoft-can-a-university-of-applied-sciences-or-university-do-the-same/

175 DGFiP, Poste de travail Linux: état de l'art et conduite du changement, published July 2024 under Creative Commons CC BY-SA 2.0 licence, in OpenDocument format. Produced under the interministerial open-source software support market, piloted by the DGFiP. Functional arbitration matrix distinguishing generalisable

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

workloads, workloads requiring case-by-case analysis, and genuine current blockers. Available via code.gouv.fr and ADULLACT. Primary commentary: ADULLACT, Poste de travail Linux, les conclusions de la DGFiP partagées, 2024, https://adullact.org/breves/67-actualite/actu-libre-france/1211-poste-de-travail-linux-les-conclusions-de-la-dgfip-partagees

176 Union delegation records, interministerial working group on information systems (GT-SI), April 2025. Confirmed full deployment of Windows 11 baseline across DGFiP workstations. Reported in: CFTC Finances Publiques, *L'informatique à la DGFiP en surchauffe*, December 2024, https://www.cftc-dgfip.fr/linformatique-a-la-dgfip-en-surchauffe/

177 CFDT Finances Publiques and CFTC Finances Publiques, joint statement, April 2025. Hardware-incompatible workstations being decommissioned rather than repurposed under Linux, despite application decoupling work completed during the study. Reported in: CFDT Finances Publiques, *Informatique à la DGFiP: grandes ambitions mais avec quels moyens?*, April 2025, https://finances.cfdt.fr/sinformer/actualites-dgfip/informatique-a-la-dgfip-grandes-ambitions-mais-avec-quels-moyens

178 Tomasz Blanc, DGFiP, interview, *IT For Business*, February 2026. Direct statements on the absence of Microsoft Office and Active Directory from the DGFiP workstation environment, default open-source stack for new projects, and NUBO sovereign cloud. Available at: https://www.itforbusiness.fr/tomasz-blanc-dgfip-au-coeur-de-letat-nous-sommes-une-administration-regalienne-du-numerique-100859

ANNEX C - Vendor evaluation criteria

Vendor evaluation framework for sovereign digital services procurement

Eight criteria. The first three are binary, and eliminatory for sensitive workloads. The remaining five are scored.

Criterion 1 - Ultimate ownership and jurisdiction (eliminatory)

Question: Who is the ultimate parent company, and in which country is it incorporated?

A provider or any entity in its direct ownership chain incorporated in the United States is subject to the CLOUD Act regardless of where data is physically stored or which entity holds the contract. This is the operative mechanism documented throughout section 2 of this report. No contractual data residency clause overrides it. Verify the complete ownership chain, not the immediate contracting entity. For providers incorporated outside the EU but not in the United States, apply the same analysis for the relevant extraterritorial jurisdiction. Treat ownership as a live variable and verify it at procurement and at every renewal cycle. The Solvinity case (section 1.4) established the mechanism.

Criterion 2 - Cloud security certification (eliminatory for sensitive workloads)

Question: Which third-party cloud security certification does the provider hold, and does it cover the specific service being procured?

SecNumCloud 3.2 (ANSSI) is the most demanding European certification currently operational and is the eligibility requirement for French sensitive public sector cloud procurement. BSI C5 (Germany) is the German federal reference. ISO 27001 is a minimum baseline but does not address sovereignty or extraterritorial jurisdiction. A provider that holds only ISO 27001 has not demonstrated compliance with European sovereignty requirements. Verify that the certification covers the specific service being procured, not only the provider's general infrastructure. A managed

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Kubernetes service that runs on a SecNumCloud-qualified IaaS layer is not itself SecNumCloud-qualified unless the managed layer has been separately assessed.

Criterion 3 — Contractual data residency (eliminatory) Question: Does the contract specify named data centre locations, and does any change require explicit customer consent?

"European data residency" as a marketing claim requires contractual specificity to be meaningful. The contract must name the data centres by country and facility. A general commitment to "EU-based processing" that can be varied unilaterally by the provider upon notice does not constitute a residency guarantee. Require that the contract prohibit transfer of data outside the named locations without explicit written consent, and that violation of this clause constitutes a material breach.

Criterion 4 — Portability and exit (scored) Question: In what format is data exported on contract termination? What is the documented process and timeline? Does the provider comply with Data Act Article 25 switching assistance obligations?

The export format must be open, documented, and interoperable: proprietary export formats that require the provider's own tooling to parse are not portability. The timeline should be 30 days or less as a contractual maximum, not a service-level objective. The cost should be zero for the data export itself. A provider that cannot specify these terms in the contract has not resolved its portability obligation. Score: 0 (proprietary format, no documented process) to 3 (open format, contractual 30-day maximum, zero cost, Data Act Article 25 explicitly referenced).

Criterion 5 — Upstream infrastructure dependencies (scored) Question: On what infrastructure does this service run? Does the provider depend on American cloud infrastructure, CDN, DNS, or AI services for the delivery of the procured service?

A European cloud provider that runs its managed services on top of AWS or Azure has not eliminated the CLOUD Act exposure it purports to replace. Ask directly and require a documented answer: on what physical infrastructure, under what jurisdiction, is this service delivered? A provider that declines to answer has not demonstrated operational sovereignty. Score: 0 (runs on American hyperscaler infrastructure) to 3 (owns its own physical infrastructure, EU-incorporated, no material American upstream dependencies).

Criterion 6 — Acquisition risk (scored) Question: Who are the investors? Does the contract include a change-of-control clause conferring termination rights if ownership changes?

A change-of-control clause should give the contracting organisation the right to terminate without penalty if the provider's ownership structure changes in a way that fails Criterion 1. Without this clause, a procurement decision that is valid at signing can become a jurisdiction dependency within the contract term. Score: 0 (no change-of-control clause, opaque investor structure) to 3 (change-of-control clause with explicit termination rights, full investor disclosure, EU-majority ownership structure).

Criterion 7 — Support location and incident handling (scored) Question: Where is support located? Are the SLA commitments contractually binding?

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Support operations located outside the EU are subject to non-EU jurisdiction for operational information exchanged during incident response. For sensitive environments, require EU-located first- and second-line support. Verify that SLA commitments are contractually binding rather than service-level objectives: a contractual SLA creates liability for non-performance; a service-level objective does not. Score: 0 (non-EU support, non-binding SLA) to 3 (EU-located support, contractually binding SLA with named escalation contacts and financial penalties for breach).

Criterion 8 — Financial viability (scored) Question: What is the provider's revenue trajectory, primary funding source, and degree of control over its own physical infrastructure?

A sovereign provider that is acquired or ceases operations mid-contract is not sovereign for the duration of that contract. The three indicators most predictive of operational continuity are: revenue growth (the provider is not dependent on continuous venture capital rounds for operational costs), funding structure (public investment, profitable operations, or long-duration committed capital rather than short-duration venture rounds), and ownership of its own physical infrastructure (a provider that rents its capacity from a third party has an additional operational dependency layer). Score: 0 (pre-revenue or operationally dependent on short-duration VC, no owned infrastructure) to 3 (profitable or backed by committed long-duration capital, owns or has long-term contracts on its own infrastructure).

Using the framework

Criteria 1, 2, and 3 are eliminatory for sensitive workloads: a provider that fails any of them should not be selected for sensitive public sector procurement regardless of its scores on the remaining criteria. For standard workloads, the eliminatory threshold can be applied with discretion based on the data classification of the workload being procured.

Criteria 4 through 8 are scored 0 to 3. A minimum aggregate score of 10 out of 15 is a reasonable baseline for any provider in a contested sovereign procurement. The threshold can be raised for mission-critical or classified workloads.

The framework applies to the initial procurement decision. It must be reapplied at each renewal cycle. Criteria 1, 3, and 6 are the highest-priority verifications at renewal: ownership, residency guarantees, and acquisition risk are the three dimensions most likely to have changed since the original assessment.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

European Digital Dependencies. Diagnosis and Priorities for Public Sector Decision-Makers
Nicolas Roux, roux.nse@proton.me, First edition, March 2026.
DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ANNEX D - Full European alternatives table by layer

Full European Alternatives Table by Layer

European Digital Dependencies: A Layer-by-Layer Assessment for Public Sector Decision-Makers

Ownership status and maturity ratings reflect the state of the market as of the publication date of this report. Verify at each procurement and renewal cycle.

Ownership legend

European - no non-EU parent identified No non-EU parent identified as of report date.

⚠️ Flag Non-EU ultimate parent or untested legal claim - verify independently at procurement and at each renewal.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.1 - Cloud Infrastructure and Compute (IaaS)						
OVHcloud	France	European - no non-EU parent identified	Bare-metal, VMs, object storage, managed Kubernetes, SecNumCloud-qualified IaaS. 43 data centres globally.	Production	SecNumCloud 3.2 (ANSSI), ISO 27001, HDS, PCI-DSS. Largest EU cloud by revenue (≈ €900 M, 2024).	Ontario court ruling (2024) subjected OVHcloud to Canadian jurisdiction for data stored in France; under appeal. Does not affect EU operations under French law. Verify at each renewal.
Scaleway	France	European - no non-EU parent identified	GPU compute, managed Kubernetes, object storage, bare metal. Primary infrastructure partner for Mistral AI.	Production	ISO 27001, HDS, PCI-DSS.	Subsidiary of Iliad Group (Xavier Niel). Strong EU governance; no non-EU parent identified.
Hetzner	Germany	European - no non-EU parent identified	Bare metal, VMs, object storage, managed load balancers. Exceptional price-to-performance ratio.	Production	ISO 27001. Widely used in EU public sector and developer workloads.	No managed AI/ML or serverless services. Suitable for standard compute and storage.
IONOS	Germany	European - no non-EU parent identified	Enterprise VMs, managed Kubernetes, object storage, managed databases, dedicated server hosting.	Production	ISO 27001, BSI C5, PCI-DSS. Subsidiary of United Internet AG (German-listed).	United Internet AG is publicly listed in Germany; no non-EU controlling shareholder identified.
T-Systems / Open Telekom Cloud	Germany	European - no non-EU parent identified	Broad managed services catalogue: VMs, storage, managed databases, container orchestration, network services. Sovereign cloud options for German federal and Länder public sector.	Production	BSI C5, ISO 27001, BSI IT-Grundschutz. Subsidiary of Deutsche Telekom AG.	Deutsche Telekom AG is ≈ 31% owned by the German federal government. Verify shareholder structure at renewal.
STACKIT	Germany	European - no non-EU parent identified	Enterprise cloud with full EU data isolation. VMs, managed Kubernetes, object storage, managed databases.	Production	ISO 27001, BSI C5. Internal cloud arm of Schwarz Group (Lidl / Kaufland).	Schwarz Group is a private German company. No non-EU parent. Growing adoption in retail, logistics, and public sector.
Cloudferro	Poland	European - no non-EU parent identified	Government and scientific cloud. EO data hosting. IaaS, object storage, HPC.	Production	ISO 27001, ISO 27017. Hosts ESA and EU Copernicus Sentinel Hub.	Specialised in public sector and scientific use cases. Limited managed services for general enterprise workloads.
Exoscale	Switzerland	⚠️ Owned by A1 Digital → A1 Telekom Austria → América Móvil	IaaS, VMs, managed Kubernetes, object storage, GPU instances. EU data centres (CH, DE, AT, BG).	Production	ISO 27001, ISO 27017, ISO 27018, FINMA, TISAX.	Markets itself as GDPR-compliant. Ultimate parent is a Mexican telecommunications group. Sovereignty claim requires independent legal verification. Apply ownership test at procurement.

		(Mexico). Non-EU ultimate parent.				
UpCloud	Finland	European - no non-EU parent identified	IaaS: VMs, managed Kubernetes, object storage, managed databases, load balancers. 13 data centres across 4 continents including 7 in Europe (DE, ES, NL, PL, SE, FI).	Production	ISO 27001, ISO 14001, CISPE member. 100% uptime SLA.	Finnish private company. Narrower service catalogue than OVHcloud or Scaleway; covers core IaaS workloads.
Aruba Cloud	Italy	European - no non-EU parent identified	VMs, managed Kubernetes, object storage, cloud backup. Data centres in IT, CZ, FR, DE, PL, UK.	Production	ISO 27001, ISO 27017, ISO 27018, CISPE founding member.	Strong Southern European presence. UK data centre is post-Brexit; verify jurisdiction requirements if used.
Leaseweb	Netherlands	European - no non-EU parent identified	Bare metal, VMs, private cloud, CDN, managed hosting. Data centres in NL, DE, and global.	Production	ISO 27001, NEN 7510 (Dutch healthcare).	Dutch private company. Broad managed hosting portfolio; less cloud-native than Scaleway or UpCloud.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.2 - Identity, Authentication and Access Management (IAM)						
Keycloak (community build)	EU / CNCF	Open source - CNCF / Linux Foundation. No corporate owner.	SSO, OAuth 2.0, OpenID Connect, SAML 2.0, MFA, user federation, fine-grained access control, passkeys (v26.4). Scales to 2,000 logins/sec on Kubernetes.	Production	CNCF incubating project. Production-proven at scale in EU government agencies, banks, large enterprises.	Self-hosting requires dedicated IAM engineering capacity. B2B federation with partner organisations running Entra ID remains a structural residual dependency.
Keycloak (Red Hat build)	USA / EU	⚠️ Red Hat owned by IBM (US). Enterprise support track is subject to US jurisdiction.	Same capabilities as community build plus enterprise support, hardened releases, CVE SLA.	Production	Red Hat Enterprise support.	Software itself is open source (Apache 2.0). Use community build + European-managed hosting for full ownership clarity.
Inteca (managed Keycloak)	Germany	European - no non-EU parent identified	Fully managed Keycloak-as-a-Service. Operations, HA, patching, monitoring, configuration included.	Production	German-incorporated independent company. No non-EU shareholder identified.	Verify ownership at each renewal: European ownership is a live variable (cf. Solvinity case, section 1.4).
Cloud-IAM (managed Keycloak)	France	European - no non-EU parent identified	Managed Keycloak SaaS. Infrastructure hosted on Scaleway (French). French jurisdiction.	Production	French-incorporated. Infrastructure on French cloud. No non-EU shareholder identified.	Same ownership monitoring caveat. Verify at each renewal.
Clever Cloud (Keycloak hosting)	France	European - no non-EU parent identified	PaaS platform supporting managed Keycloak deployment among other services.	Production	French-incorporated, Nantes-based. No non-EU shareholder identified.	PaaS provider, not a Keycloak specialist. Suitable for organisations with internal IAM engineering capacity seeking European hosting.
LemonLDAP::NG	France	Open source - OW2 consortium (French public sector).	SSO/IdP for web applications. SAML 2.0, OAuth 2.0, OpenID Connect, 2FA. Citizen-facing and internal public sector use cases.	Production	OW2 open-source consortium. ANSSI-referenced. Widely deployed in French public administration.	Better suited to web SSO and citizen-facing authentication than to full enterprise IAM at scale. Complement to Keycloak.
RCDevs (WebADM)	Luxembourg	European - no non-EU parent identified	Multi-factor authentication, identity management, RADIUS, OTP, FIDO2. On-premises deployment with offline functional continuity. Federates with Entra ID and Keycloak.	Production	Luxembourg private company. GDPR-compliant. Deployed in European regulated sectors.	Complement to Keycloak for MFA and on-premises authentication resilience. Positioned for NIS2 offline functional continuity requirements.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.3 - Endpoint Security and Threat Detection (EDR / XDR)						
HarfangLab	France	European - no non-EU parent identified	EDR: process tree analysis, file, network, memory monitoring. Cloud, hybrid, on-premises, SecNumCloud deployment modes.	Production	Full ANSSI qualification (Jan 2025). BSI BSZ (Germany, 2025) - first EDR with dual FR-DE government certification.	Telemetry scale smaller than CrowdStrike/SentinelOne. Gap is manageable for most EU public sector threat profiles.
Tehtris	France	European - no non-EU parent identified	Full XDR: endpoint, network, email, cloud. Automated neutralisation without human intervention. Honeypot and deception capabilities.	Production	ANSSI-referenced. Deployed in European gov. and critical infrastructure.	Primarily XDR rather than pure EDR. Stronger in automated response than in deep forensic investigation workflows.
Sekoia.io	France	European - no non-EU parent identified	XDR / SIEM / CTI platform. Integrates natively with HarfangLab, Stormshield, Tehtris as endpoint agents.	Production	ANSSI-approved. Frost & Sullivan XDR Leader 2023. Gartner emerging technology 2024.	Requires an EDR agent for endpoint coverage. Best combined with HarfangLab or Tehtris for full European stack.
Stormshield Endpoint	France	European - subsidiary of Airbus (Franco-German defence group).	Endpoint protection for highly regulated environments: defence, critical infrastructure, ICS/SCADA. Air-gapped and classified support.	Production	ANSSI-qualified. EAL3+ Common Criteria. NATO Restricted-grade deployments.	Airbus is a Franco-German listed company; no non-EU controlling shareholder. Strong for defence/critical infrastructure; less suited to general administration.
WithSecure Elements	Finland	European - no non-EU parent identified	Cloud-delivered EDR with full GDPR compliance, European data residency, managed detection and response option.	Production	AV-TEST Advanced EDR certification 2024 (100% detection). Spun out of F-Secure enterprise division 2022.	Upstream threat intelligence feeds may partially source from non-European providers, as with all EDR vendors.
ESET	Slovakia	European - no non-EU parent identified	AV, EDR, full endpoint protection. Broad OS coverage. Widely deployed in EU public sector.	Production	GDPR-compliant. European data centres. Slovak private company (founder-controlled).	Less specialised for SOC/advanced threat detection than HarfangLab or Sekoia. Strong baseline protection.
Bitdefender GravityZone	Romania	European - no non-EU parent identified	EDR, XDR, managed detection. Strong automated threat response. European data centres.	Production	Consistently strong AV-TEST and AV-Comparatives scores.	Private equity involvement in shareholder structure - verify current ownership at procurement. Romanian founder retains majority control as of this report.
WithSecure Elements	Finland	European - no non-EU parent identified	EDR/XDR: behavioural analytics, automated response, managed detection option. European data residency. Cloud-delivered. Full MITRE ATT&CK evaluation participation.	Production	Gartner Magic Quadrant Visionary 2025 (one of two EU-HQ vendors). AV-TEST Advanced EDR certified 2024 (100% detection).	Spun out of F-Secure enterprise division (2022). Finnish private company. Upstream threat intelligence feeds may partially source from non-EU providers, as with all EDR vendors.
ESET	Slovakia	European - no non-EU parent identified	AV, EPP, EDR (ESET Inspect), full endpoint protection. Broad OS coverage (Windows, macOS, Linux). On-premises and cloud deployment. Strong Central/Eastern European public sector presence.	Production	MITRE ATT&CK evaluated. Deployed in EU public sector. On UK Digital Marketplace (G-Cloud).	Founder-controlled Slovak private company (founded 1992). One of the oldest European cybersecurity companies. Less specialised for advanced SOC workflows than HarfangLab or Sekoia; strong baseline protection at scale.
Bitdefender GravityZone	Romania	European - no non-EU parent identified	EDR, XDR, managed detection and response. Automated threat response, cloud sandboxing. European data centres. Public sector and enterprise focus with NIS2/GDPR compliance positioning.	Production	Consistently strong AV-TEST and AV-Comparatives scores. Public sector cybersecurity solutions.	Romanian founder retains majority control as of report date. Private equity involvement in shareholder structure — verify current ownership at procurement.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.4 - Productivity and Collaboration						
Nextcloud Hub	Germany	European - no non-EU parent identified	File storage, collaborative document editing (Collabora Online), video conferencing (Talk), messaging, calendar, email. Self-hostable or managed via European partners.	Production	Deployed in hundreds of EU government organisations. EDPS, Austrian BMWET (2025), German public sector. ISO 27001.	Managed service layer at large public sector scale (50k+ users) is maturing but not yet as standardised as Microsoft 365.
Collabora Online	UK / Germany	European - no non-EU parent identified	Browser-based collaborative office document editing (Writer, Calc, Impress). Strong MS Office format compatibility. Default document engine in Nextcloud Hub and OpenDesk.	Production	LibreOffice-based (The Document Foundation). Used in Schleswig-Holstein, ICC migration (2025).	Edge-case MS Office format fidelity issues persist for complex macros and legacy VBA workflows. UK company; not subject to US extraterritorial law.
Open-Xchange	Germany	European - no non-EU parent identified	Email, calendar, contacts, tasks, groupware. Used as email backend in Schleswig-Holstein (40k mailboxes, Oct 2025).	Production	ISO 27001. Deployed in large EU carrier and public sector email migrations.	Primarily a groupware/email backend; combine with Nextcloud for file storage and Collabora for document editing.
LibreOffice	Germany	Open source - The Document Foundation (German non-profit).	Full desktop office suite: Writer, Calc, Impress, Draw, Base, Math. ODF native, MS Office format support.	Production	ODF ISO standard. Deployed in Gendarmerie Nationale (103k workstations), Schleswig-Holstein, numerous EU administrations.	Desktop application; not browser-based collaborative editing. Combine with Collabora Online for web workflows.
Matrix / Element	UK	⚠️ Element Ltd is a UK company. Protocol is open and fully self-hostable with no dependency on Element Ltd.	Open federated messaging protocol. Self-hostable. E2E encryption. Used by German Bundeswehr, French Tchap (375k MAU), multiple EU government deployments.	Production	Matrix.org Foundation (non-profit). Multiple EU government deployments documented.	A self-hosted Matrix deployment (Synapse/Dendrite) on EU infrastructure has no dependency on Element Ltd. Sovereignty is complete when self-hosted.
Jitsi Meet (self-hosted)	USA / self-hosted	⚠️ 8x8 Inc. (US) maintains the upstream. Self-hosted open-source deployments are independent of 8x8.	Open-source video conferencing. Self-hostable. France's earlier webconf.numerique.gouv.fr was Jitsi-based and is being decommissioned. France's current Visio service is built on LiveKit (see section 2.4). Self-hosted Jitsi remains a viable alternative for organisations not using the Suite Numérique.	Production	Apache 2.0 licence. Widely deployed in EU public sector self-hosted instances.	Use self-hosted instances exclusively. Using meet.jit.si (8x8 cloud) creates a US dependency that eliminates sovereignty entirely.
Open-Xchange (OX App Suite)	Germany	European - no non-EU parent identified	Email, calendar, contacts, tasks, groupware. Full CalDAV/CardDAV/ActiveSync. WebUI and native mobile clients. Modular architecture for carrier and public sector deployment.	Production	GPLv2 backend. Deployed at Schleswig-Holstein (40,000 mailboxes, Oct 2025). Widely deployed by European telecoms as managed email backend.	Primary use case is groupware backend for hosters and public sector. Combine with Nextcloud for file storage.t this report does not
CryptPad	France	European - no non-EU parent identified	End-to-end encrypted collaborative editing: documents, spreadsheets, presentations, kanban, forms. Zero-knowledge architecture: server cannot read content.	Production	Developed by XWiki SAS (France). Funded by EU research grants (NGI). GDPR-compliant by architecture.	Encryption architecture means the server operator cannot read document content. Relevant for classified or legally privileged material. Smaller feature set than Nextcloud/Collabora for general productivity.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.5 - Payments and Financial Transactions						
SEPA / EBA Clearing	EU institutional	European institutional - governed by ECB and European banking consortium.	SEPA Credit Transfer and SEPA Instant (< 10 seconds, mandatory eurozone since Jan 2025). Exclusively European clearing. No American intermediary.	Production	EU PSD2/PSD3. 88% of euro-area participants registered for Instant as of early 2026.	Bank-to-bank transfers only. No card scheme, no consumer wallet. Structurally resilient to any American network-level decision.
Wero / EPI	EU (FR, DE, BE, NL…)	European - consortium of 16 major European banks. €500 M capitalisation. European Commission supported.	Consumer digital wallet on SEPA Instant rails. Account-to-account in < 10 seconds. Bypasses Visa/Mastercard entirely. E-commerce live in Germany (Nov 2025). 48.5 M registered users (early 2026).	Production (P2P) Emerging (merchant)	PSD2-compliant. Apple NFC ruling (Jul 2024) enables tap-to-pay on iPhone. EuroPA Alliance MoU (130 M users, 13 countries).	Merchant acceptance outside Germany nascent. Physical card layer abandoned. Restricted to 16 founding banks. Full parity with Visa/Mastercard is 2-3 years away. Residual: Google Play Integrity API for Android payments.
Worldline	France	European - no non-EU parent identified	End-to-end payment processing, acquiring, card issuing, POS terminals, digital payments. Large EU public sector and retail footprint.	Production	PCI-DSS Level 1. French publicly listed company.	European acquirer and processor; not a card network. Visa/Mastercard network authorisation still routes through those networks for card transactions.
Adyen	Netherlands	European - no non-EU parent identified	Omnichannel payment processing, acquiring, issuing. Strong e-commerce and enterprise focus.	Production	PCI-DSS Level 1. Dutch publicly listed company.	Same Visa/Mastercard network dependency as Worldline for card transactions.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.6 - Content Delivery, Visibility and Distribution (CDN / DNS / DDoS)						
Bunny.net	Slovenia	European - no non-EU parent identified	CDN, DNS, object storage, video delivery, DDoS protection (basic-to-mid tier), WAF. 119 PoPs globally. Average latency 24 ms vs Cloudflare 28 ms.	Production	GDPR-compliant. Slovenian private company. Serves 1 M+ websites. Migration from Cloudflare documented at < 2 hours for standard deployments.	No Cloudflare-equivalent Zero Trust, full enterprise WAF, or email security. Adequate for CDN/DNS for majority of EU public sector use cases. Does not match Cloudflare's hyper-volumetric DDoS absorption for nation-state-grade attacks.
Gcore	Luxembourg	European - no non-EU parent identified	CDN, DDoS protection (1.5 Tbps), edge computing, cloud (VMs, managed Kubernetes, GPU). Enterprise-grade security.	Production	Luxembourg-incorporated private company. GDPR-compliant. ISO 27001.	DDoS capacity (1.5 Tbps) is significant but below Cloudflare's scale for the largest hyper-volumetric attacks.
KeyCDN	Switzerland	European - no non-EU parent identified	Core CDN, HTTP/2, image processing, EU data centres, GDPR-compliant.	Production	Swiss private company. No non-EU parent identified.	Basic CDN only. No DDoS protection beyond HTTP-layer filtering. Switzerland is not EU but not subject to US extraterritorial law.
Qwant	France	Qwant's partial ownership by Axel Springer SE (majority-held by KKR, US private equity) applies the ownership flag. Search engine at below 1% market share. See section 2.6 for the strategic implications.	European privacy-respecting search engine. French language strength. Below 1% of European search market. Included here to document the absence of a viable European general search alternative, not as a procurement option.	Maturity: **Not viable. Included for completeness**	French data residency. GDPR-compliant.	Holds < 1% of European search market. KKR (US PE) holds majority of Axel Springer, which holds a stake in Qwant - verify current ownership structure independently.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.7 - Artificial Intelligence and Data Processing						
Mistral AI (API)	France	⚠️ French private company. Microsoft holds a €15 M convertible note (Feb 2024). NVIDIA compute dependency. Verify convertible note status at procurement.	LLMs (Mistral Large 3, Mistral Small 3.1, Magistral). Open-weight and API access. Native EU AI Act compliance. French government framework agreement.	Production	ISO 27001, ISO 27701, SOC 2 Type II. €11.7 B valuation (Sep 2025).	Use Mistral's own API (French jurisdiction, no training data use) not Azure AI Studio (US jurisdiction, CLOUD Act exposure). Self-hosted open-weight models provide full sovereignty.
Mistral AI (self-hosted open-weight)	France	European - no non-EU parent identified	Mistral open-weight models self-deployed on European IaaS. Data never leaves the organisation's perimeter.	Production	Apache 2.0 licence. No API dependency, no data egress, full jurisdictional sovereignty.	Requires internal AI engineering capacity or a European managed inference provider. GPU compute dependency on NVIDIA hardware remains at infrastructure layer.
Aleph Alpha (Luminous)	Germany	European - no non-EU parent identified	Explainable LLMs for regulated and government use cases. On-premises and sovereign cloud deployment. German-language and multilingual support.	Production	Deployed in German federal agencies and Bundeswehr. GDPR-compliant.	Specialised for explainable AI in regulated sectors; narrower capability breadth than Mistral's model family.
Pleias (formerly LightOn)	France	European - no non-EU parent identified	Open language models trained on curated multilingual European corpora. Focus on document AI, RAG, enterprise search.	Emerging	French private company. Open model weights. GDPR-compliant.	Smaller models optimised for document and enterprise search. Complementary to Mistral for document-centric workflows.
European managed inference	N/A	N/A - market gap as of this report.	No European provider currently offers a fully managed AI inference platform with SLA guarantees, GDPR contractual guarantees, audit trails, and enterprise support, at the scale required for large public sector procurement.	Gap	-	Use Mistral's own API rather than Azure AI Studio. The managed service wrapper required for standard public sector procurement without internal AI engineering capacity does not yet exist at production scale.

Provider	Country	Ownership	Core capabilities	Maturity	Certifications / deployments	Caveats and residual dependencies
Layer 2.8 - Software Development and Delivery Infrastructure						
Forgejo / Codeberg	Germany	Open source - Codeberg e.V. (German non-profit). GNU GPL. No corporate owner.	Git hosting, issue tracking, pull requests, Forgejo Actions (CI/CD), package registry, container registry. Hard fork of Gitea under fully European non-profit governance.	Production	Codeberg e.V. is a German registered non-profit. Strongest sovereignty story in this layer.	CI/CD capability covers standard workflows; lacks GitLab's integrated DevSecOps depth (SAST, DAST, container scanning as native features).
GitLab Community Edition (self-hosted)	USA (corporate) open source	⚠️ GitLab Inc. is US-incorporated. Self-hosted CE eliminates CLOUD Act exposure for hosted data, but software is developed under US corporate governance.	Full DevSecOps: Git hosting, CI/CD, container registry, package registry, SAST, DAST, dependency scanning, issue tracking. Most functionally complete self-hosted alternative to GitHub.	Production	MIT licence (CE). Deployed in German federal Open CoDE platform, numerous EU administrations.	Strongest feature set. US corporate governance is a partial limitation. For maximum governance sovereignty, prefer Forgejo.
Woodpecker CI	EU / open source	Open source - Apache 2.0. Community-governed fork of Drone CI. No corporate owner.	CI/CD pipeline engine. Self-hostable. Integrates with Forgejo, Gitea, GitLab, GitHub as repository backends.	Production	Community-maintained. Used in European open-source and public sector CI deployments.	Less feature-rich than GitLab CI for complex pipelines. Suitable for standard build-test-deploy workflows.
Sonatype Nexus OSS (artifact proxy)	USA (corporate) open source	⚠️ Sonatype is US-incorporated. OSS edition is Apache 2.0 and fully self-hostable with no runtime dependency on Sonatype infrastructure.	Self-hostable artifact repository and package proxy. Caches npm, PyPI, Maven, Docker Hub locally. Internal security scanning before packages enter the pipeline.	Production	Apache 2.0 (OSS edition). Widely deployed in enterprise DevSecOps stacks.	Resolves build-time resilience dependency on upstream registries in disruption scenarios. Does not replace upstream registries; caches them. Governance dependency on American-controlled upstreams persists at systemic level.
European sovereign registries (gap)	N/A	N/A - does not yet exist at scale.	Independent European registries with their own governance, maintainer identity infrastructure, package signing, and supply chain security tooling, capable of serving as primary publication endpoints.	Gap (3-5 yr horizon)	-	Internal proxies (e.g. Nexus OSS) resolve build-time resilience at organisational level within normal budgets in weeks. European upstream registries with independent governance require institutional commitment and maintainer adoption. Achievable within 3-5 years; structurally less constrained than semiconductor sovereignty or subsea cable governance.

How to read this table

This annex is a companion to the layer-by-layer dependency mapping in section 2.

Ownership entries flagged ⚠️ indicate a non-EU ultimate parent or a material ownership risk requiring independent legal verification. The flag does not mean the provider is unusable; it means the dependency audit must account for it explicitly.

Maturity: Production (operationally proven at public sector scale), Emerging / Pilot (in active development or early deployment), or Gap (no credible European alternative currently exists at the required level).

A provider that passes the ownership test at procurement may be acquired by a non-European entity before the next renewal. Verify ownership at each cycle. The mechanism is documented in section 1.4.

This table does not substitute for a procurement-grade technical assessment. Consult ENISA's EUCS catalogue, ANSSI's SecNumCloud list, France's SILL, Germany's Open CoDE, and the Interoperable Europe Portal for current certification and deployment status.

Providers deliberately excluded

S3NS (Thales + Google Cloud): SecNumCloud 3.2 qualified (Dec 2025). ANSSI's Director General stated CLOUD Act immunity is valid 'in principle' - untested under adversarial conditions. Not a substitute for European-owned platforms when full jurisdictional certainty is required.

Bleu (Orange + Capgemini + Microsoft): Targeting SecNumCloud qualification H1 2026. Same structural logic as S3NS applied to the Microsoft Azure platform. Same untested legal engineering caveat.

Silo AI (Finland): Acquired by AMD (US) in 2024. Removed from the European sovereign ecosystem by the ownership test applied in this report.

Exoscale: Included in the IaaS table with an ownership flag. Ultimate parent is América Móvil (Mexico). Listed because infrastructure is European and GDPR-compliant; ownership chain must be acknowledged explicitly.

Qwant: Included in the CDN/search table with an ownership flag reflecting partial ownership by Axel Springer, itself majority-held by KKR (US private equity).

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ANNEX E - Key initiatives and organisations to follow

This annex is a reference tool, not an endorsement. Each entry is included because it is operationally relevant to the dependency landscape mapped in this report and is likely to produce developments worth monitoring over the coming two to three years. Entries are organised by function, not by quality.

The information in this annex reflects the state of these initiatives as of March 2026. Given the pace of change in this domain, direct verification against current sources is recommended before any operational use.

European institutional initiatives

Digital Commons EDIC (DC-EDIC) Established by European Commission decision on 29 October 2025, officially launched in The Hague on 11 December 2025. Founding members: France, Germany, the Netherlands, Italy. Observer and candidate members: Luxembourg, Slovenia, Poland, Belgium. Statutory seat in Paris. Mandate: jointly develop, deploy, and operate cross-border open-source digital infrastructure in the areas of AI, cloud, cybersecurity, geomatics, and public administration tools. Software developed under DC-EDIC defaults to free and open-source licences. By 2027: one-stop-shop and expertise hub, annual State of the Digital Commons report. The most structurally significant new European digital sovereignty instrument created since Gaia-X, and deliberately designed to avoid Gaia-X's governance failure by excluding commercial hyperscalers from its governance structure.

Interoperable Europe Board Established under the Interoperable Europe Act (Regulation EU 2024/903). First meeting December 2024; mandatory interoperability assessments applicable as of January 2025. Primary venue for influencing the open protocol mandates described in section 4.2. Public consultation calendar available at interoperable-europe.ec.europa.eu.

ENISA (European Union Agency for Cybersecurity) Designated implementing body for the EUCS certification framework. Primary source for tracking the status of EUCS negotiations and the Cybersecurity Act revision. Publishes annual threat landscape reports, cloud security guidelines, and NIS2 implementation guidance. enisa.europa.eu.

European Payments Initiative / Wero The most significant European payment sovereignty development currently in active deployment. 48.5 million registered users as of early 2026; merchant payments live in Germany, France and Belgium following in 2026; EuroPA Alliance MOU signed February 2026 covering 130 million users across 13 countries. Progress toward full pan-European merchant acceptance is the variable to monitor. eupaymentsinitiative.eu.

National programmes with European transferability

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ZenDiS (Centre for Digital Sovereignty of Public Administration located in Germany) Develops and maintains openDesk, the open-source office suite deployed by Schleswig-Holstein and the International Criminal Court. Implementing partner for Germany in DC-EDIC. Primary reference for any administration considering an openDesk deployment. zendis.de.

Sovereign Tech Agency (Germany) Provides public investment in the maintenance and security of open-source infrastructure components. Co-architect of DC-EDIC's governance model. The closest European equivalent to a public interest foundation for digital infrastructure. sovereign.tech.

DINUM (Direction Interministérielle du Numérique located in France) Operates the Suite Numérique, maintains code.gouv.fr, the French public sector open-source software catalogue, and pilots interministerial open-source support markets. Primary national reference for French public administrations. numerique.gouv.fr.

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information located in France) Maintains SecNumCloud 3.2, the most technically rigorous cloud security certification in Europe. Publishes the list of qualified providers, security advisories, and the CSPN/qualification framework for cybersecurity products including EDR platforms. The primary French reference for any public sector security procurement decision. ssi.gouv.fr.

BSI (Bundesamt für Sicherheit in der Informationstechnik located in Germany) German federal cybersecurity authority. Maintains its own cloud security framework and IT baseline protection catalogues. Operates mutual recognition agreements with ANSSI that underpin the dual French-German certifications documented in section 2.3. bsi.bund.de.

Open CoDE (Germany) Federal platform for publishing and reusing public administration software. Primary German reference for open-source deployment documentation, including BundesMessenger and the software components underlying DC-EDIC projects. opencode.de.

code.gouv.fr (France) French public sector open-source software catalogue and repository, maintained by DINUM. Hosts the DGFiP Linux workstation study and migration documentation from French public administrations. code.gouv.fr.

Industry and civil society

Hexatrust French and European association of cybersecurity and trusted cloud providers. Members include HarfangLab, Tehtris, OVHcloud, Clever Cloud, and other European providers assessed in this report. Primary supply-side advocacy body for European sovereign technology in French and European regulatory processes. hexatrust.com.

CIGREF Association of large French and European organisations on digital transformation, with members spanning both public and private sectors including Airbus, AXA, BNP Paribas, and major French public institutions. Published the €264 billion European digital dependency assessment in April 2025. Co-signatory of the November 2025 joint declaration on digital sovereignty with Belgian, Dutch, and German counterparts. cigref.fr.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

EuroStack initiative An emerging coalition of European technology providers, researchers, and civil society organisations advocating for a layered European digital infrastructure strategy. Producing policy papers and convening discussions on the governance conditions required for European digital sovereignty. Worth monitoring as a developing policy voice.

Open Source Observatory (OSOR) / Interoperable Europe Portal European Commission platform cataloguing open-source solutions deployed across EU public sector organisations, with case studies and implementation documentation. References over 640 solutions across 30-plus public sector domains. interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor.

OpenForum Europe Brussels-based think tank focused on open-source policy, standards, and digital sovereignty. Produces policy analysis on EUCS, the Data Act, and cloud interoperability that is directly relevant to the regulatory levers described in section 4. openforumeurope.org.

Regulatory processes to monitor

EUCS finalisation and Cybersecurity Act revision The single most consequential pending regulatory decision for European public sector cloud procurement. The Commission's revision of the Cybersecurity Act, scheduled for 2025-2026, is the legislative vehicle. ENISA's consultation calendar and the European Parliament's ITRE committee are the primary tracking points.

eIDAS 2.0 / European Digital Identity Wallet Implementation timeline for the citizen-facing European digital identity standard. Relevant for public administrations developing citizen authentication infrastructure. Operational deployment expected from 2026 onward across member states.

PSD3 / Open Banking regulation Expected 2026. Will strengthen open banking requirements relevant to the payment layer documented in section 2.5 and the conditions under which Wero can expand merchant acceptance.

EU AI Act implementation High-risk AI system obligations become applicable in stages from 2025 onward. The governance gap between AI Act requirements and current public sector AI procurement practices is documented in section 2.7. ENISA's AI certification work and the AI Office's guidance are the primary tracking points.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

ANNEX F - European Public Sector Expenditure on American Digital Platforms

Reference figures for the financial argument. Orders of magnitude. March 2026.

Scope	Amount	Period	Source
1 - Aggregate European public sector expenditure			
Total EU public sector spend on U.S. software and services	≈ €265 billion	Annual	Open Cloud Coalition / TED analysis
European online advertising market (Google + Meta dominant share)	≈ €124 billion	Annual (2025 est.)	IAB Europe / Statista
Visa + Mastercard: annual European card payment volume processed (U.S.-controlled clearing networks)	> €7 trillion	Annual	ECB Payments Statistics 2024
2 - Country-level documented expenditure			
Germany - federal government Microsoft licences	€481 million	Annual	Bundestag parliamentary question, 2024
Germany - federal + Länder Microsoft licences (est.)	"Significantly higher"	Annual	Bundestag member statement, 2024
France - Ministry of National Education Microsoft framework contract (Crayon France, 2025-2029)	€74 M min / €152 M ceiling	4-year contract	Official procurement notice, Mar 2025
France - total public sector annual IT spend on U.S. software (est.)	≈ €10-15 billion	Annual (est.)	Cour des comptes / Open Cloud Coalition
3 - AI investment asymmetry (structural context for section 2.7)			
U.S. private AI investment	$109.1 billion	2024	Stanford AI Index 2025
EU private AI investment (estimated)	≈ $3-4 billion	2024	Stanford AI Index 2025 / EIB
U.S. / EU investment ratio	≈ 30:1	2024	Derived
U.S. vs. EU VC funds under management	$270 B vs. $44 B	2024	NVCA / Invest Europe
4 - Documented migration savings (reference cases for the financial argument)			
Case	**One-time cost**	**Annual savings**	**Payback**
Schleswig-Holstein (30,000 employees - email + full office suite, Oct 2025)	€9 million	> €15 million	< 1 year
Gendarmerie Nationale (103,000 workstations - full desktop migration, 2005-2014)	Not published	≈ €2 M/yr licences; TCO −40%	Cumul. ≈ €50 M

€265 billion aggregate figure.
Covers all U.S. software and services purchased by European public organisations. Derived from Open Cloud Coalition modelling of Tenders Electronic Daily procurement data. Covers professional cloud computing and software services. American companies capture approximately 80% of EU spending in this category, a sum the authors describe as comparable in scale to Europe's annual energy import bill. Derived from Asterès modelling of EU spending data, commissioned by Cigref and Numeum, April 2025 (https://www.cigref.fr/technological-dependence-on-american-software-and-cloud-services-an-assessment-of-the-economic-consequences-in-europe).

€7 trillion card payment volume.
Included as a scale indicator, not a cost figure: it quantifies the share of European payment flows subject to American network-level control (Visa and Mastercard clearing infrastructure), and therefore the scope of the payment sovereignty dependency discussed in section 2.5.

Germany and France procurement figures.
Sourced from official parliamentary and procurement documents. Precise.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Schleswig-Holstein savings figure.
The most directly usable benchmark for decision-makers constructing a business case. One-time cost: €9 million. Annual savings from 2026: > €15 million. Payback: under one year.

AI investment asymmetry.
Included to contextualise the structural conditions producing American AI dominance documented in section 2.7. The 30:1 ratio is the mechanism, not a grievance.

ANNEX G - Priority decisions for European-scale action

This annex is addressed to senior policymakers, parliamentarians, and Directors-General seeking a consolidated view of the four decisions that would materially change the dependency landscape documented in this report. Each entry identifies the institutional owner, the current blocker, and the signals that would indicate genuine progress. The full analytical basis for each decision is in Section 4.

Decision 1 - Establish sovereignty criteria as binding eligibility thresholds through the CADA, sectoral mandates, and national certification frameworks

What the decision is: Sectoral mandates (NIS2, DORA, health data regulation) + CADA legislative process + national certification frameworks (SecNumCloud, C5, ENS).

Institutional owner: European Commission (DG CONNECT), with ENISA as implementing body. The Cybersecurity Act revision provides the legislative vehicle. Member state consensus is required in the Council; the ITRE committee of the European Parliament is the primary scrutiny venue.

Current blocker: Sovereignty criteria removed from EUCS scheme under documented industry lobbying pressure. CADA instrument pending, binding force and eligibility threshold design undetermined at publication date.

Progress signals: CADA publication and legal structure. Member state coalition positions on sovereignty thresholds. UGAP Nuage Public contract award as operational precedent. Formal ENISA mandate to begin provider assessments against the finalised scheme within six months of adoption. A Commission technological sovereignty package is expected in May 2026 and is described as including sovereign cloud infrastructure provisions and supply chain cybersecurity liability for digital infrastructure.[112] Its formal publication and the presence or absence of binding sovereignty criteria will be the first concrete test of Commission intent following the EUCS setback.

Realistic horizon: 2026, contingent on the CSA revision timeline and member state consensus. The Franco-German bilateral commitment of November 2025 is the most direct available lever for building that consensus.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

Decision 2 - Mandate open interoperability protocols through the Interoperable Europe Board

What the decision is: Extend the Interoperable Europe Board's current mandate to cover three specific protocol requirements for all European public administrations: Matrix-compatible federation endpoints for inter-organisational messaging, ODF as the default format for cross-border administrative document exchange, and OpenID Connect-compatible endpoints for B2B identity federation between public bodies.

Institutional owner: The Interoperable Europe Board, established under Regulation EU 2024/903. The Board held its first meeting in December 2024 and issued binding interoperability assessment guidelines in January 2025. No new legislative vehicle is required; the Board's existing mandate covers cross-border public sector interoperability. DG DIGIT is the Commission service responsible.

Current blocker: The Board's current guidelines cover general interoperability assessment methodology. They do not yet mandate specific protocol standards at the collaboration and identity federation layers. Extending the mandate to cover these layers requires a Board decision, not new legislation, but requires political support from member state representatives on the Board.

Progress signals: A Board recommendation specifically naming Matrix, ODF, and OpenID Connect as mandatory protocol standards for public sector procurement. Inclusion of protocol compliance as a scored criterion in cross-border interoperability assessments. Adoption of ODF mandate in at least three additional member states beyond those already implementing it.

Realistic horizon: 2026 for the Board recommendation, 2027-2028 for meaningful implementation across member state administrations.

Decision 3 - Establish a joint procurement framework for sovereign digital services

What the decision is: Create an EU-level pre-qualification catalogue for EUCS-certified European digital service providers, structured on the FedRAMP model, eliminating per-organisation security assessment costs and creating the aggregated demand signal that European providers require to invest at scale. Coordinate member state procurement volumes through a joint framework modelled on the European Defence Agency's joint procurement architecture.

Institutional owner: European Commission (DG GROW and DG CONNECT jointly), with the Publications Office administering the pre-qualification catalogue. The EDA joint procurement model requires a Council decision to extend to digital services. UGAP in France and the Beschaffungsamt in Germany are the national procurement bodies whose existing frameworks are the most directly usable building blocks.

Current blocker: The absence of a finalised EUCS (Decision 1) means there is no harmonised certification standard against which a pre-qualification catalogue can be built. Decisions 1 and 3 are sequentially dependent: the procurement framework requires the certification framework. A joint

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0

procurement framework built before EUCS finalisation would reproduce the fragmentation it is designed to address.

Progress signals: A Commission communication establishing the pre-qualification catalogue as a policy objective linked explicitly to the EUCS finalisation timeline. Bilateral Franco-German agreement on a shared procurement lot for at least one layer (cloud IaaS or EDR) as a pilot. Inclusion of sovereignty criteria as mandatory scored elements in at least one major EU framework contract renewal (European Commission's own cloud procurement is the highest-visibility available test case).

Realistic horizon: 2027 at the earliest, contingent on EUCS finalisation in 2026.

Decision 4: Mandate the DC-EDIC to define layer-by-layer workload portability floors

What the decision is: Direct the Digital Commons EDIC to produce, within 24 months of its operational launch, binding technical specifications for minimum workload portability at four layers: cloud infrastructure, identity and access management, collaborative document exchange, and AI inference. Commit founding member states to translating those specifications into procurement eligibility conditions within their national frameworks within 12 months of DC-EDIC publication.

Institutional owner: DC-EDIC Governing Board (founding members: France, Germany, the Netherlands, Italy). The statutory seat is Paris; ZenDiS (Germany) is the primary implementing partner. The DC-EDIC's mandate already covers the relevant technical domains. This decision requires a resolution of the DC-EDIC Governing Board, supported by political commitment from the digital ministries of the four founding states.

Current blocker: The DC-EDIC was launched in December 2025 and its work programme is not yet public. The risk is scope diffusion: an institution with a broad mandate and limited initial capitalisation will gravitate toward the technically accessible rather than the strategically necessary. A specific mandate for portability floor specifications, adopted by the Governing Board within the first operational year, would prevent that drift.

Progress signals: Publication of a DC-EDIC work programme that explicitly includes portability floor specifications for each of the four layers. A Governing Board resolution committing to completion within 24 months. At least one founding member state incorporating a DC-EDIC portability specification into a live procurement process before the full set is complete.

Realistic horizon: Portability specifications published by end of 2027. National procurement integration by 2028-2029.

The four decisions are not independent. Decision 1 (sovereignty certification thresholds) is the precondition for Decision 3 (joint procurement). Decision 4 (DC-EDIC portability floors) reinforces Decision 2 (interoperability mandates) at the technical layer. The Franco-German bilateral axis is the most direct available instrument for building the member state consensus that all four require. Progress on any one decision creates political and institutional momentum for the others.

DOI: https://doi.org/10.5281/zenodo.19358628 - CC BY 4.0