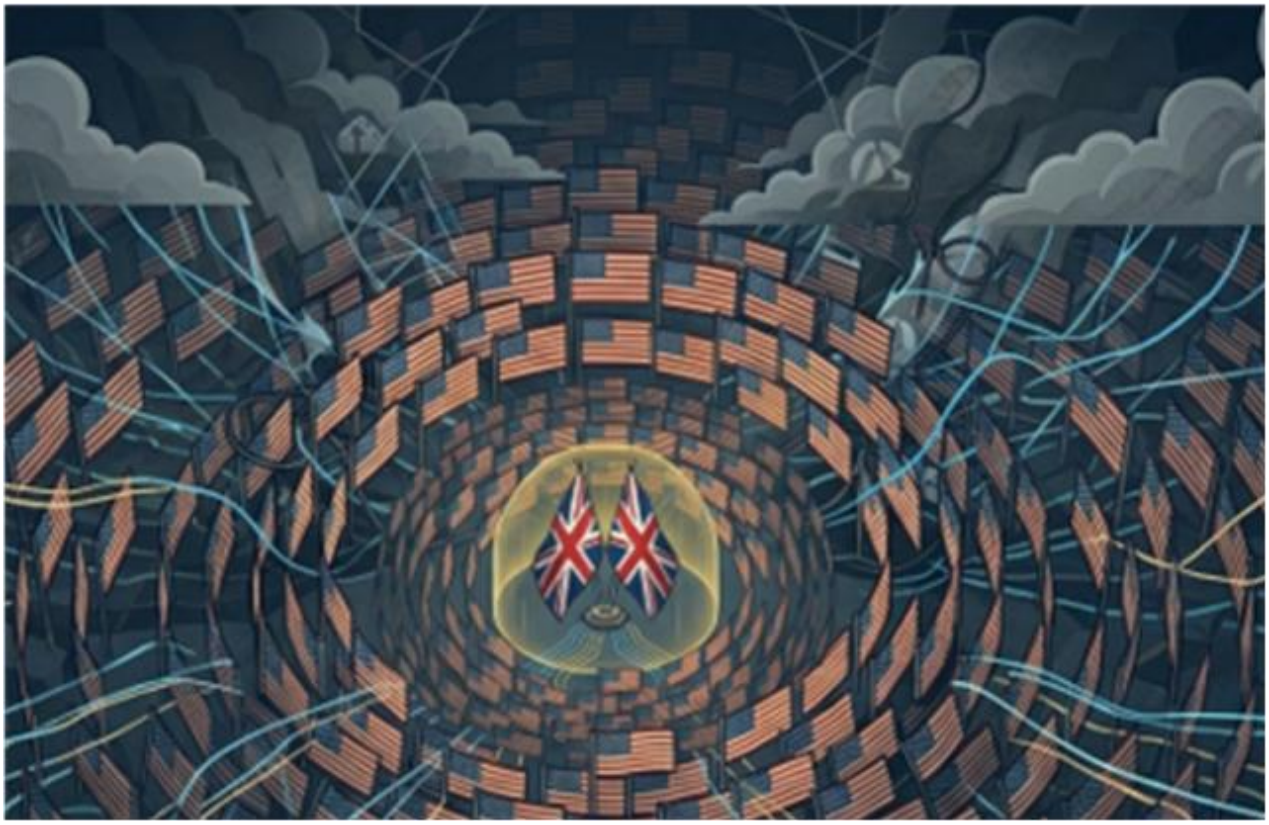
Europe's Shift to Non-US Cyber Products

Encouraging, Initiating and Mandating of Sovereign Substitutes

Contents



1. Executive Summary

Since early 2025, and accelerating through 2026, European governments have moved from rhetorical support for “digital sovereignty” toward concrete policy instruments, such as certification regimes, procurement mandates, direct capital, and in one case outright supplier exclusion. All aimed at reducing structural dependence on US-headquartered cybersecurity, cloud, and productivity vendors.

The trigger set is consistent across capitals: exposure of EU/UK data to the US CLOUD Act and FISA 702; a run of politically charged incidents, including Microsoft's suspension of International Criminal Court officials' email accounts following US sanctions and concern over potential US leverage tied to the Greenland dispute; and continuing US hyperscaler concentration, with American providers holding roughly 70% of the European cloud infrastructure market against a European share of around 15%. Gartner tracks European sovereign-cloud infrastructure spend rising from $6.9bn in 2025 to a projected $23.1bn by 2027.

The response is uneven. France has gone furthest, embedding sovereignty requirements into law through ANSSI's SecNumCloud certification and the “Cloud au Centre” doctrine. Poland has moved fastest and hardest in 2026, pairing a NIS2 transposition with a law empowering regulators to exclude “high-risk” and non-NATO suppliers outright. Germany's push is substantial but fragmented, led by individual Länder rather than the federal government, though it has now reached the Chancellery. Denmark has moved quickly at ministry and municipal level. The Netherlands, Italy and Spain are proceeding mainly through certification and impact-assessment frameworks rather than substitution mandates. The Nordics and Baltics favour open standards, budget signalling and “EU-only” tender clauses over binding law. The United Kingdom, despite parliamentary recognition of the dependency risk, remains the most passive of the major economies reviewed: it has no procurement mandate favouring non-US suppliers.

At EU level the picture is genuinely split. The European Commission has funded a sovereign cloud procurement framework and proposed a revised Cybersecurity Act built around ICT supply-chain risk, but it has explicitly stripped “sovereignty requirements” (jurisdictional immunity, non-EU ownership caps) from the EU-wide cloud certification scheme (EUCS) after sustained industry and member-state disagreement. That retreat at the supranational level has left individual capitals, led by France and now Poland, to set the pace unilaterally, producing a genuinely fragmented, multi-speed European sovereignty landscape rather than a single EU policy.

2. Strategic Drivers

Legal exposure: the US CLOUD Act allows US authorities to compel US-headquartered providers to hand over data regardless of where it is physically stored, an exposure contractual assurance cannot fully remove.

FISA Section 702 raises parallel concerns for EU/UK public-sector and critical-infrastructure data.

Precedent shocks: Microsoft's suspension of ICC officials' email accounts after US sanctions, and concern in Denmark over potential US pressure connected to Greenland, have been cited directly in UK and Nordic policy debate as evidence that vendor dependency can translate into political leverage.

Market concentration: US hyperscalers account for roughly 70% of European cloud infrastructure spend and are collectively investing on the order of $600bn in cloud and AI infrastructure in 2026, dwarfing the European sovereign-cloud base even as that base triples in size.

Regulatory stacking: NIS2, DORA, the EU Data Act's switching/portability provisions, and national schemes (SecNumCloud, ENS, BSI C5) increasingly compound, turning vendor-nationality and jurisdictional-immunity questions into board-level compliance issues rather than IT preferences.

Political signalling: in November 2025 all 27 EU member states signed a declaration on the “shared ambition to strengthen Europe's digital sovereignty” and reduce strategic dependencies. This was a rhetorical high-water mark that individual states are now converting into national law at very different speeds.

3. The EU-Level Framework: Funding and Rhetoric ahead of Law

The European Commission's own posture illustrates the tension running through this briefing: it is willing to fund and coordinate sovereignty but has so far declined to mandate it at supranational level, leaving hard exclusion mechanisms to national capitals.

October 2025: the Commission's corporate IT service published a Cloud Sovereignty Framework with an eight-point definition and scoring formula for EU institutional procurement (not binding on the wider private market).

April 2026: the Commission awarded a €180m six-year sovereign cloud contract to a consortium of four European providers: Luxembourg's Post Telecom, Germany's STACKIT, France's Scaleway and Belgium's Proximus, to serve the Commission, Parliament and Council.

January 2026: The Commission proposed a revised Cybersecurity Act establishing an EU-wide ICT supply-chain security framework for critical sectors and enabling mandatory assurance levels. Legal analysis shows that the CSA2 package *does not amend NIS2* and *does not exclude sovereignty criteria*; instead, sovereignty protections are reintroduced through the EUCS High+ tier and the companion Cloud & AI Data Act, including safeguards against third-country extraterritorial access for the highest-assurance use cases.

The EUCS cloud-certification scheme, in development since 2019, has been effectively stalled since 2024: successive drafts stripped out “immunity from non-EU law” and ownership-cap provisions after objections from the US government, US industry associations and several member states, to the visible frustration of sovereignty advocates such as the European DIGITAL SME Alliance; individual states, above all France, continue to apply national sovereignty requirements regardless.

The Cloud and AI Development Act (CADA), expected in the first half of 2026, is intended to create a formal four-level sovereignty assurance framework for highly critical public-sector cloud and AI workloads.

This is the clearest sign that binding EU-level sovereignty criteria may yet re-emerge, having been removed from EUCS.

4. Country-by-Country Analysis

Each entry below classifies the government's posture as Encouraging (soft guidance, funding, or market signalling), Initiating (formal programmes or pilots without a binding legal mandate), or Mandating (a binding legal or procurement requirement favouring non-US or EU-controlled suppliers), and lists recent, dated examples of substitution activity.

France

Posture: **Mandating, the most advanced and legally binding regime in Europe**

Lead institution(s): ANSSI (national cybersecurity agency); Ministry for Public Accounts and Reform

Recent examples

ANSSI's SecNumCloud v3.2 certification is mandatory, under the “Cloud au Centre” doctrine, for French state administrations and “Operators of Vital Importance” handling sensitive data and imposes explicit non-EU ownership caps (below 25% individually, 39% collectively, with no non-EU board veto) that structurally exclude standard US hyperscaler offerings.

US hyperscaler technology can only reach SecNumCloud-gated workloads through majority-French joint ventures: Bleu (Orange/Capgemini, distributing Microsoft Azure, qualification pending) and S3NS (Thales-majority, with Google as a capped minority partner), which secured SecNumCloud 3.2 qualification in December 2025 and now serves reference customers including EDF, Qonto and Thales itself.

April 2026: the government announced migration of roughly 2.5 million civil-service desktop computers from Microsoft Windows to Linux, alongside an existing commitment to replace Zoom and Microsoft Teams with the French-built Visio platform across government departments by end-2027.

Mandatory HDS health-data certification, tied to SecNumCloud, has been written into recent tenders such as the national Health Data Hub, explicitly excluding standard foreign cloud offerings from handling sensitive health data.

Germany

Posture: **Initiating state-led and fast-growing, now reaching the federal executive**

Lead institution(s): State (Länder) digital ministries; ZenDiS (federal Centre for Digital Sovereignty)

Recent examples

Schleswig-Holstein is migrating roughly 30,000 civil servants from Word, Outlook and SharePoint to LibreOffice, Thunderbird and Open-Xchange (plus a Nextcloud rollout and a Linux pilot), reporting 80% completion by mid-2026 at a one-off €9m cost against roughly €15m in annual Microsoft licensing.

Mecklenburg-Vorpommern is deploying a Nextcloud-based sovereign collaboration platform, run by state IT provider DVZ M-V, targeting more than 50,000 public-sector employees for file-sharing, chat, video and groupware, replacing Microsoft SharePoint-equivalent tooling.

Chancellor Friedrich Merz's own Chancellery has begun shifting from Microsoft 365 to openDesk, a “sovereign by design” suite built by ZenDiS. This is the clearest sign the substitution movement has reached the federal executive rather than remaining confined to individual states.

Private capital is reinforcing the state-level push: Schwarz Gruppe (Lidl's parent company) has committed €11bn to its own sovereign cloud provider, STACKIT, which also won a share of the EU institutions' €180m sovereign cloud procurement.

Bavaria is reported to be evaluating comparable Microsoft alternatives, suggesting the state-by-state pattern is still spreading rather than consolidating into a single federal mandate.

Denmark

Posture: **Mandating at ministry and municipal level; fast, explicit, but reversible in tone**

Lead institution(s): Ministry of Digital Affairs

Recent examples

The Ministry of Digital Affairs announced in mid-2025 a phased move off Microsoft 365 and Windows, piloting the open-source suite Collabora (based on LibreOffice) inside its F2 case-management system from June 2025, with the minister framing dependence on “very few foreign suppliers” as a financial and strategic vulnerability.

Copenhagen and Aarhus, Denmark's two largest municipalities, announced Microsoft phase-outs ahead of the national ministry, citing cost, market dominance, and political tension with Washington with commentary at the time linking the move explicitly to concern over US leverage in the Greenland dispute.

The programme is explicitly reversible: Minister Caroline Stage has said the ministry could revert to Microsoft “in an instant” if the open-source transition proves too complex, marking Denmark's approach as a determined but pragmatic pilot rather than an irreversible legal mandate.

Poland

Posture: **Mandating; the newest and legally hardest-edged regime in Europe**

Lead institution(s): Ministry of Digital Affairs; national cybersecurity system under the amended KSC Act

Recent examples

April 2026: Poland's amended Act on the National Cybersecurity System (KSC Act), transposing NIS2, extended binding supply-chain security obligations to suppliers across critical sectors including energy, transport and manufacturing.

A separate law signed by President Nawrocki in mid-2026, after an earlier veto, explicitly targets “non-NATO suppliers” and gives regulators power to designate and eliminate “high-risk suppliers” from critical infrastructure and telecoms. This is the most forceful outright-exclusion mechanism identified among the countries reviewed, echoing but broadening the earlier Huawei/5G precedent.

A €700m “cybershield” investment in critical-infrastructure protection was announced amid escalating Russian-linked attacks, including a December incident that reportedly brought the national power grid close to a blackout, and following reports that Poland suffered the highest volume of cyberattacks of any EU state in the prior year.

The Ministry of Digital Affairs is separately preparing a “technological sovereignty test” for major public-sector technology purchases (reported July 2026), assessing data control and vendor dependency for large IT projects. Officials frame this as informed choice rather than isolation, with a five-year target to retain more domestic value in cloud and software spend.

Netherlands

Posture: **Encouraging / conditional; impact-assessment-driven rather than a blanket mandate**

Lead institution(s): Dutch data protection authorities; municipal digital-strategy units

Recent examples

Dutch government agencies have conducted formal Data Protection Impact Assessments (DPIAs) on Microsoft 365 and Google Workspace, resulting in binding compliance conditions and, in specific cases, mandated migration to European alternatives; a conditional, case-by-case approach rather than an outright ban.

Amsterdam published a Multiyear Digital Autonomy Strategy 2026–2035, targeting full municipal digital sovereignty by 2035. This is among the most explicit long-horizon city-level commitments identified in this review.

NIS2 and Critical Entities Resilience (CER) compliance deadlines are pushing the Dutch identity and access-control market toward vendors that combine sovereign-cloud hosting with GDPR-native architectures, though large US IAM/PAM incumbents (Okta, SailPoint, CyberArk) remain heavily represented at Dutch identity-industry events, indicating substitution pressure has not yet displaced US vendors from the core IAM/PAM category.

Italy

Posture: **Encouraging / institutional; comprehensive strategy, procedural rather than substitutional**

Lead institution(s): ACN (Agenzia per la Cybersicurezza Nazionale)

Recent examples

ACN, established in 2021, is executing Italy's National Cybersecurity Strategy 2022–2026 (82 measures across three objectives), which includes a specific mandate to define qualification criteria for cloud infrastructure and providers used by public administration as a certification-led lever rather than an explicit vendor-substitution order.

Italian public institutions have been named, alongside Austria, Denmark and Germany, among those piloting LibreOffice and open-source alternatives to Microsoft's office suite.

2026: ACN signed a formal collaboration agreement with Spain's INCIBE to develop joint cybersecurity capacity-building and industrial/research synergies, signalling a preference for EU-level coordination over unilateral national mandates.

Spain

Posture: **Encouraging / institutional; certification and domestic-capability funding**

Lead institution(s): INCIBE (private sector / citizens); CCN-CERT (public administration)

Recent examples

The Esquema Nacional de Seguridad (ENS) certification is mandatory at Basic, Medium or High levels for ICT systems used by Spanish public administrations Spain's equivalent of Germany's BSI C5 or France's SecNumCloud, though ENS does not carry SecNumCloud's explicit non-EU ownership exclusions.

NIS2 has been transposed via the Ley de Coordinación y Gobernanza de la Ciberseguridad (LCyGC), introducing personal board- and CISO-level liability for cybersecurity governance failures and a dual-authority compliance model.

The 'Digital Spain 2026' strategy (axis 04, measure 16) sets an explicit goal of positioning Spain as an international cybersecurity hub, and INCIBE has separately run a €96m EU-funded pre-commercial procurement programme funding domestic solutions for botnet detection, ransomware monitoring, fraud detection and SOC tooling direct investment in indigenous capability rather than a displacement mandate.

Nordics & Baltics (Finland, Sweden, Estonia)

Posture: **Encouraging; market-signalling and open standards over binding law**

Lead institution(s): Finnish and Swedish national cybersecurity authorities; Estonian Ministry of Digital Affairs

Recent examples

Finland: growing “EU-only vendor eligible” clauses in public and managed-service tenders are credited by industry analysts with driving concrete partner wins for the Finnish cybersecurity vendor WithSecure, including telecom operator DNA and several Dutch managed-service providers a rare, named, contract-level example of policy-linked substitution benefiting a specific European vendor.

Sweden: NIS2 transposition (March 2024 guideline) extended cybersecurity obligations to roughly 3,000 additional entities; Swedish procurement increasingly favours identity tooling integrated with the national BankID scheme as a domestic-sovereignty anchor for authentication.

Estonia: Digital Minister Pakosta has explicitly rejected reliance on “closed, proprietary black-box” solutions in favour of open-source sovereign digital-state infrastructure, backed by an increased 2026 state-budget allocation built on Estonia's long-standing X-Road e-government architecture rather than a new substitution programme.

Austria adopted a national charter on digital sovereignty in 2025, later folded into the EU-wide declaration signed by all 27 member states, and Austrian institutions are separately named among those piloting LibreOffice migration.

United Kingdom

Posture: **Encouraging only; the most passive posture among the major economies reviewed**

Lead institution(s): NCSC; DSIT (including the Sovereign AI unit); Cabinet Office (GovAssure)

Recent examples

No procurement mandate favouring non-US or UK/EU-controlled cyber suppliers is currently in force. Existing levers Cyber Essentials Plus (now mandatory under G-Cloud 15, with an April 2026 reset requiring MFA and barring end-of-life software) and GovAssure/the NCSC Cyber Assessment Framework set security baselines rather than vendor-nationality requirements.

The Cyber Security and Resilience Bill (introduced 12 November 2025; second reading 6 January 2026; Royal Assent expected 2026 with phased implementation to 2028) will create a "designated critical suppliers" regime with enhanced obligations.

5. Assessment: Ranking Government Activism

The ranking below weighs four factors observed across the evidence: (i) whether the mechanism is legally binding or merely encouraged; (ii) whether it explicitly excludes or disadvantages non-EU/non-UK ownership rather than simply requiring good security practice; (iii) scale of committed funding and users affected; and (iv) how recently and how fast the posture has hardened. On this basis, France and Poland stand apart as the only governments operating genuinely binding exclusion mechanisms; the United Kingdom is the clear outlier at the passive end among the major economies.

Rank	Country	Posture	Basis for ranking
1	France	Mandating (binding)	Only regime with a hard legal gate (SecNumCloud) carrying explicit non-EU ownership caps for public procurement and critical-sector data; longest track record (since 2016); national-scale desktop OS migration announced in 2026.
2	Poland	Mandating (binding, newest)	2026 law empowers outright exclusion of "high-risk" and non-NATO suppliers from critical infrastructure the hardest-edged mechanism reviewed; backed by €700m of committed funding and a sovereignty test in preparation.
3	Germany	Initiating, state-led, now federal	Large committed budgets and user counts at state level (Schleswig-Holstein, Mecklenburg-Vorpommern) plus €11bn private capital behind STACKIT; has now reached the federal Chancellery via openDesk but still lacks a single national legal mandate across all 16 Länder.
4	Denmark	Mandating at ministry/municipal	Explicit, dated ministerial decision plus the two largest municipalities acting ahead of it; smaller in absolute scale than France or Germany and explicitly framed as reversible.
5	Netherlands	Encouraging / conditional	DPIA-driven restrictions create real substitution pressure, and a 2035 municipal strategy (Amsterdam) shows ambition, but no blanket national mandate; US IAM/PAM vendors remain prominent in the domestic market.
6	Spain	Encouraging / institutional	Mandatory ENS certification and NIS2 transposition build compliance architecture and fund domestic capability (€96m INCIBE programme), but do not exclude US vendors outright.
7	Italy	Encouraging / institutional	Comprehensive national strategy and a qualification mandate for public-sector cloud, but procedural in character; formal preference for EU-level coordination (Spain cooperation agreement) over unilateral substitution.
8	Finland & Nordics	Encouraging / market-led	"EU-only" tender clauses are demonstrably shifting named contracts to domestic vendors (WithSecure) but operate case-by-case rather than through a national mandate.
9	Estonia & Baltics	Encouraging / architectural	Strong open-source and sovereignty rhetoric with increased budget commitment but built on a pre-existing e-government architecture rather than a new substitution programme.
10	United Kingdom	Encouraging only (least active)	Security-baseline and supply-chain-resilience legislation (Cyber Essentials Plus, GovAssure, the CSR Bill) acknowledges dependency risk in principle but contains no procurement mandate favouring non-US suppliers.

6. Outlook and Implications

Fragmentation is likely to persist rather than converge: the EU's retreat from binding sovereignty criteria in EUCS means national law, not EU law, will keep setting the pace. France's SecNumCloud model and Poland's supplier-exclusion law are the most likely templates for other states to adapt.

Watch the Cloud and AI Development Act (expected H1 2026) closely: it is the most plausible route for binding sovereignty criteria to re-enter EU law after being stripped from EUCS and would materially raise the floor for all 27 member states at once.

Hybrid “sovereign-by-JV” structures (Bleu, S3NS, and the STACKIT/Schwarz Gruppe model) are emerging as the practical compromise wherever full displacement of US technology is not feasible so expect this pattern to spread beyond France and Germany as other states seek scale without full technical replacement.

Germany's trajectory (state pilots → ZenDiS → the Chancellery) is the clearest evidence that state- or agency-level pilots can escalate into national policy within 18–24 months; Poland's 2026 acceleration suggests the same pattern can move even faster once a hybrid-threat trigger (the December power-grid incident) is present.

The UK is the most exposed of the major economies to being left behind: its own parliamentary analysis already documents the dependency risk in detail, but translating the Cyber Security and Resilience Bill's supply-chain provisions into an explicit sovereignty or substitution mandate would require a policy step the government has not yet taken.

Page down for sources.

7. Sources

All sources accessed August 2026. Listed by first relevant use in the briefing; publication dates as reported by each outlet.

Cloud Security Alliance, “EU Tech Sovereignty: Cloud Concentration Risk and the Compliance Cascade,” June 2026.

GovInfoSecurity, “Europe Spurs Digital Sovereignty With $213M Cloud Contract,” 17 April 2026.

Broadcom, “Three Predictions for Sovereign Cloud in 2026,” 2026.

MassiveGRID, “Why European Companies Are Leaving US Cloud Providers in 2026,” 12 March 2026.

ASEE, “EU Cloud Sovereignty: Why Businesses Are Moving Away from US Providers,” 18 May 2026.

CNBC, “Europe bids for digital sovereignty amid Russia threats, Trump,” 18 February 2026.

Digital Watch Observatory, “German state pushes digital sovereignty,” 16 September 2025.

TechCrunch, “What's behind Europe's efforts to ditch US software in favor of sovereign tech,” 27 April 2026.

Cybernews, “German state replaces Microsoft with open source, saves millions each year,” 8 December 2025.

Cybernews, “Another German state is replacing Microsoft with open-source software,” 3 July 2026.

The Register, “Another German state heads down the open-source sovereignty road,” 8 July 2026.

Irish Times, “A small German state's quiet revolt against Microsoft and what it means for Europe,” 14 February 2026.

Tuta, “France ditches Microsoft for Linux to achieve digital sovereignty,” 2 July 2026.

6clicks, “NIS2 + DORA + SecNumCloud: The 2026 wake-up call for French GRC,” 29 May 2026.

ITIF, “France's Cloud Service Restrictions,” 25 May 2025.

Chambers and Partners, “Cybersecurity 2026 France,” 17 March 2026.

Cross-Border Data Forum, “‘Sovereignty Requirements' in France and Potentially EU Cybersecurity Regulations.”

The Record (Recorded Future News), “Danish government agency to ditch Microsoft software,” 13 June 2025.

How-To Geek, “LibreOffice Is Replacing Microsoft 365 in Denmark's Government,” 2025.

cBrain, “The Ministry of Digital Affairs launches a pilot project on digital sovereignty,” 19 June 2025.

Computer Weekly, “Campaigners urge UK to develop digital sovereignty strategy.”

Civo, “UK Sovereign Cloud Security Standards to Watch in 2026,” 21 April 2026.

iProov, “UK Cyber Action Plan 2026: Identity Verification Impact,” 29 May 2026.

UK Parliament, Cyber Security and Resilience (NIS) Bill, Public Bill Committee memorandum CSRB04, 3 February 2026.

PwC UK, “Understanding The Cyber Security & Resilience Bill.”

Taylor Wessing, “UK Cyber Security and Resilience Bill: key considerations for technology businesses,” 16 March 2026.

Notes From Poland, “Poland tightens cybersecurity rules targeting non-NATO suppliers,” 22 February 2026.

Forbes, “Poland Seeks To Curb Dependence On Big Tech With ‘Sovereignty Test',” 21 July 2026.

CMS Law, “Cybersecurity in the supply chain: what NIS2 changes in Poland,” 10 April 2026.

INCIBE, “Spain and Italy sign collaboration agreement to boost European cybersecurity.”

sota.io, “Spain NIS2 Implementation 2026 INCIBE-CERT, CCN-CERT & SaaS Compliance Guide.”

R Street Institute, “Cybersecurity Score European Cybersecurity Certification Scheme For Cloud Services (EUCS).”

Clifford Chance, “EU cyber reforms proposed, including overhauled Cybersecurity Act,” February 2026.

Mayer Brown, “European Commission Proposes Major Cybersecurity Package to Strengthen EU Cyber Resilience,” 9 March 2026.

INCYBER NEWS, “Bleu and S3NS, the ‘sovereign' cloud offerings from Microsoft and Google.”

Futurum Group, “S3NS Analyst Summit 2026 Unveils Sovereign Cloud Roadmap,” 5 March 2026.

Forrester (via forrester.com), “S3NS Summit Highlights Sovereignty And Trusted Cloud Progress.”

Simply Wall St, “European Digital Sovereignty Tailwinds Will Support This Cybersecurity Provider's Long-Term Upside Potential” (WithSecure), 8 January 2026.

Vocal/Trader, “Netherlands Access Control Market 2026,” 19 May 2026.