The Double Structure of Digital Sovereignty

Europe's Departure from Palantir and the Chains of American Big Tech

Kim Kyung-jin · Attorney at Law

Table of Contents

1.1 The Decision of France's General Directorate for Internal Security (DGSI): Transition to ChapsVision's ArgonOS

France's General Directorate for Internal Security (DGSI) was established in 2014 by reorganizing the existing organization that handled domestic intelligence. Its mission is to monitor terror threats and respond to foreign espionage and cyberattacks. The DGSI has used Gotham, a data analytics program from the American company Palantir, since 2016. The impetus for its adoption was the November 2015 terror attacks in Paris. The DGSI urgently needed a tool to examine the communication records, movement routes, and financial flows of terrorist organizations on a single screen, and Palantir's program filled that role.

The French government did not leave this dependence unaddressed from the start. In 2021, the Ministry of the Interior launched OTDH, a procurement project seeking technology from French companies to process vast amounts of data in different formats within a single national system. ChapsVision entered this bidding process alongside Athea—a joint venture formed by defense giant Thales and IT company Eviden—and software company Blueway. However, none of the candidates established themselves quickly enough to take over the DGSI's daily operations entirely.

Behind the DGSI's decision to partner with Palantir again in December 2025 was the reality that alternative technology had not yet fully taken root in the field.

On December 15, 2025, Palantir announced that it had renewed its multiyear contract with the DGSI. It was a three-year contract. Less than six months after signing the new deal, in June 2026, the French government made a decision that directly conflicted with this contract.

The catalyst was an action by the U.S. government. On June 9, 2026, American artificial intelligence company Anthropic released Fable 5 and Mythos 5, its most advanced models. Just three days later, at 5:12 p.m. Eastern Time on June 12, the U.S. government issued an export control directive citing national security to immediately suspend foreign nationals' access to Fable 5 and Mythos 5. Because there was no rapid way to verify user nationality, Anthropic chose to temporarily block access for all overseas users, including those in Europe.

European researchers and administrative agencies trying to use the newly released models found their access cut off after just three days. Although access was restored

around July 1 when export controls were lifted, European entities witnessed firsthand that an ally could sever access to core technology with a single law.

Months before this incident, the European Parliament had already set a course toward reducing technological dependence. On January 22, 2026, the European Parliament adopted a resolution on European technological sovereignty and digital infrastructure by a vote of 471 in favor, 68 against, and 71 abstentions. This resolution expressed concern over excessive reliance on a small number of foreign providers in cloud infrastructure, semiconductors, artificial intelligence, and cybersecurity, proposing the principle of prioritizing open-source software in public procurement alongside a 10-billion-euro sovereign technology fund.

France's decision came five months after the adoption of this resolution, serving as a national-level implementation case.

The French government acted after observing the situation for four days. On June 16, 2026, Prime Minister Sébastien Lecornu announced that the Palantir tools used by the DGSI would be replaced with ArgonOS from French company ChapsVision. The announcement came one day before the opening of VivaTech in Paris, Europe's largest technology exhibition. A day earlier, on June 15, ChapsVision was added to the Next40, an index of French innovative companies.

The Next40 is a support index operated by the French government since 2019, accessible only to unicorns valued at over 1 billion euros or companies that have raised more than 100 million euros in investment within three years. As the two announcements overlapped within two days, it left the impression that the decision was a plan long prepared by the government. Prime Minister Lecornu stated that France could not accept another strategic dependence in information technology, adding that the era of relying on the goodwill of allies was over.

One fact needs to be noted here: an announcement and a contract termination are not the same event. On June 17, the day after the announcement, Le Monde reported that Palantir claimed the contract renewed in December 2025 remained legally valid. The French government's public declaration of a new supplier and the actual termination of the existing contract require separate procedures. The French Ministry of the Interior also acknowledged the remaining period of the extended contract with Palantir, stating that winding down the contract requires a separate administrative process.

The actual replacement will take more time. The French Ministry of the Interior projected that deploying the new program to intelligence operations and migrating existing data would take 18 to 24 months. Other reports suggest that looking at the

overall contract structure, a complete transition will take place between 2027 and 2029. Interior Minister Laurent Nuñez promised a transition period through 2027 during which both systems would operate simultaneously to bridge this gap. The reason the migration takes so long is that it is not simply a matter of replacing a single program.

The DGSI must sequentially follow five steps: adapting established operating methods to the new interface, retraining agents, setting up new data routing paths, ensuring ongoing investigations remain uninterrupted, and verifying whether the system can handle actual workloads. DGSI agents are already accustomed to Palantir's interface layout and operating methods, and the data storage structure itself is tailored to American system standards. Because hastily severing the connection risks creating a lapse in intelligence operations, the French government chose a phased transition.

The new platform under development by ChapsVision is also set to include features where AI agents perform portions of search and analysis on behalf of users; verifying whether these features operate as reliably in actual investigative fields as Palantir's tools is another factor extending the migration period.

Underpinning this decision was the France 2030 investment plan. The government allocated an additional 655 million euros for self-reliance in artificial intelligence. A portion of this was used to develop conversational AI tools for civil servants. On June 16, 2026, Minister for Public Service David Amiel announced that the chatbot "L'Assistant," previously trialed with 10,000 users, would be expanded to all one million civil servants. The cost for the initial stage of expansion was estimated between 700,000 and 750,000 euros, with development handled by French AI firm Mistral AI.

Arthur Mensch, CEO of Mistral AI, has maintained that Europe must move away from relying on borrowed U.S. cloud infrastructure and possess its own. His remarks provided logical support for the DGSI's decision.

ChapsVision, France's new provider, was founded in 2019 by CEO Olivier Dellenbach. Dellenbach previously sold the financial analysis software company eFront to BlackRock for $1.3 billion in 2019. ChapsVision chose a strategy of expanding through acquisitions rather than internal development. After acquiring customer relationship management software company Coeris, retail data company Octipas, e-commerce company Sparkow, and marketing automation company NP6 in succession, it also acquired Bertin IT and Vequsys, which possessed cybersecurity, intelligence, and voice recognition technologies.

With the acquisitions of Bertin IT and Vequsys, revenue grew from 30 million euros to 40 million euros, and the number of employees rose from 260 to 380. After repeating

more than twenty-five such acquisitions, the company secured funding from France's public investment bank Bpifrance and Tikehau Capital, raised an additional 100 million euros in 2022, and reached 200 million euros in annual revenue in 2025.

ArgonOS, created by ChapsVision, is a software program that gathers and analyzes information of different formats in one place. It handles not only documents, but also video, audio, and open-source intelligence—meaning publicly accessible internet data—all in one place. The program runs in air-gapped environments disconnected from external networks, or on sovereign clouds managed directly by the state. European shareholders hold 100 percent of the company's equity. This ownership structure matters because of the US CLOUD Act. This law stipulates that any service operated by a US entity must hand over information upon request from US law enforcement agencies, regardless of which country the servers are located in.

Because ArgonOS is not owned by a US entity, it falls outside the scope of this law.

The process by which France's General Directorate for Internal Security (DGSI) selected ChapsVision also warrants examination. The company went through the bidding process for OTDH, a data integration project launched by the French Ministry of the Interior in 2021. OTDH is an initiative aimed at processing vast amounts of heterogeneous data within a single national system, with a total budget set at approximately 40 million euros. After more than three years of evaluation, ChapsVision won the Lot 1 contract to organize raw data at the end of 2024. Competition for Lot 2 was even fiercer.

In the final stage for this lot, three contenders remained: Athea, a joint venture between Thales and Eviden; software company Blueway; and ChapsVision. ChapsVision won this competition as well in June 2026, securing the Lot 2 contract to visualize data and build models, becoming the final winning bidder. With this award, ArgonOS established itself as the foundational system handling data processing not only for the DGSI but across multiple judicial and law enforcement agencies.

France's decision also influenced neighboring countries. Germany's Federal Office for the Protection of the Constitution (BfV) confirmed its decision to adopt the same ArgonOS in May 2026, ahead of France. The background and progress of this decision will be covered in the next section.

Completely stripping out American technology from French state institutions is not something that will be finished in a few months. The operational methods familiar to agents, data standards, and the remaining terms of existing contracts all remain obstacles. Nevertheless, the fact that the French government publicly changed course

remains unalterable. When the contract with Palantir will completely end and how smoothly the actual migration to ArgonOS will proceed remain facts to be verified in the future.

Sources and References

1. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026-06-16, https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision

2. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, https://www.businesswire.com/news/home/20251215083215/en

3. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, https://www.anthropic.com/news/redeploying-fable-5

5. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

6. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026-06-16, https://www.chapsvision.com/press-release/chapsvision-chosen-by-france-to-deploy-argonos-for-otdh-project/

7. Unknown author, 'L'Etat français déploie Mistral AI auprès d'un million de fonctionnaires', ChannelNews, 2026-06-16, https://www.channelnews.fr/letat-francais-deploie-mistral-ai-aupres-dun-million-de-fonctionnaires-et-inclut-la-souverainete-numerique-dans-les-objectifs-2026-2029-de-lugap-157317

8. BlackRock, 'BlackRock to Acquire eFront -- Industry Leading Alternatives Investment Software Provider', Business Wire, 2019-03-22, https://www.businesswire.com/news/home/20190322005228/en/BlackRock-to-Acquire-eFront----Industry-Leading-Alternatives-Investment-Software-Provider

9. Unknown author, 'DGSI : Palantir éjecté, ChapsVision prend le relais en 2029', info.fr, 2026, https://info.fr/palantir-ejecte-dgsi-france-rompt-dependance-americaine-chapsvision/

10. Unknown author, 'French Security Service to Replace Palantir With Local Software', Bloomberg, 2026-06-16, https://www.bloomberg.com/news/articles/2026-06-16/french-security-service-to-replace-palantir-with-local-software

11. Unknown author, 'ChapsVision to replace Palantir in major contract with French intelligence agency', Sifted, 2026, https://sifted.eu/articles/chapsvision-to-replace-palantir-in-major-contract-with-french-intelligence-agency

12. Unknown author, 'Quatre choses à savoir sur Palantir, ce géant technologique américain controversé qui travaille avec la DGSI', franceinfo, 2026, https://www.franceinfo.fr/societe/armee-securite-defense/quatre-choses-a-savoir-sur-palantir-ce-geant-technologique-americain-controverse-qui-travaille-avec-la-dgsi_7682872.html

13. ChapsVision, 'ChapsVision acquiert Bertin IT et Vecsys', ChapsVision, 2021, https://www.chapsvision.fr/acquisition-bertin-it-et-vecsys-par-chapsvision/

14. La mission French Tech, 'French Tech Next40/120', La mission French Tech, 2026, https://lafrenchtech.gouv.fr/en/programme/french-tech-next40-120/

15. Unknown author, 'Anthropic releases Claude Fable, a version of Mythos, days after warning AI is becoming too dangerous', TechCrunch, 2026-06-09, https://techcrunch.com/2026/06/09/anthropics-claude-fable-5-is-a-version-of-mythos-the-public-can-access-today/

16. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', European Parliament, 2026-01-22, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022_EN.html

17. GIFAS, 'Athea, ChapsVision et Blueway retenus par la DGSI pour la seconde phase du programme OTDH', GIFAS, 2026, https://gifas.fr/press-summary/athea-chapsvision-et-blueway-retenus-par-la-dgsi-pour-la-seconde-phase-du-programme-otdh

18. Author Unknown, 'La France tourne la page Palantir : ChapsVision remporte le marché de la DGSI pour sa plateforme de traitement et d'exploitation de données', Usine Digitale, 2026, https://www.usine-digitale.fr/souverainete/la-france-tourne-la-page-palantir-chapsvision-remporte-le-marche-de-la-dgsi-pour-sa-plateforme-de-traitement-et-dexploitation-de-donnees.I3EESPQQIBEX3AQXHIF6ABGI3M.html

1.2 The Departure of Germany's Federal Office for the Protection of the Constitution (BfV) and Exclusion from the Federal Defense Cloud

In Germany, the domestic intelligence agency and the military distanced themselves from Palantir at different points in time, yet in the same direction. These two decisions were not a single event, but two separate facts that went through distinct processes.

Germany's Federal Office for the Protection of the Constitution (BfV) is the top-tier agency handling domestic intelligence. Charged with monitoring extremist movements and countering foreign espionage, it occupies a position similar to France's General Directorate for Internal Security (DGSI). In December 2025, Director Sinan Selen stated at an internal German meeting that security agencies must establish a clearer European perspective and break free from long-term dependencies. In May 2026, five months after this statement, the BfV finalized its procurement of French company ChapsVision's ArgonOS instead of Palantir's program. It was recorded as the first instance of a German federal agency officially rejecting Palantir.

ArgonOS, chosen by the BfV, is the same program described in the previous section. It integrates and analyzes information in different formats, and also features open-source intelligence capabilities that track publicly available internet information. The noteworthy aspect on the German side is the partnership formed during the actual deployment of this program. ChapsVision joined hands with ROLA Security Solutions, an information technology company that has long managed Germany's police database, PIAV. By collaborating with a firm already established within the German law enforcement network, they ensured the new program could be smoothly overlaid onto the existing system.

This procurement will not lead to immediate field deployment. The German federal government is preparing a legislative amendment spanning over 700 pages to redefine the powers of the Federal Intelligence Service (BND) and the BfV. This amendment grants both agencies the authority to intervene directly in threat situations along with new tools for handling artificial intelligence and biometric data, while mandating information sharing among the BfV, state intelligence agencies, and the Military Counterintelligence Service (MAD). As the Federal Constitutional Court of Germany set the deadline for this legislative revision at the end of 2026, the Bundestag will take up the bill immediately after the summer recess.

New analytical tools, including ArgonOS, can only become fully operational once this legal framework is established. Without the law yet in place, the agency must navigate a transition period while maintaining existing systems. The confirmation of procurement and the moment that procurement goes live are thus tied to distinct procedural timelines.

Apart from the BfV's decision, the Bundeswehr took separate steps to exclude Palantir from the military domain. In 2017, the Bundeswehr established a separate military branch called the Cyber and Information Domain Service, assigning it sole responsibility for cyber defense and the operation of information systems. Vice Admiral Thomas Daum, commander of this service, stated in an interview with the German financial daily Handelsblatt on April 28, 2026, that there were currently no plans whatsoever to use Palantir in military cloud projects. He remarked that granting employees of a foreign private company access to Germany's national data was unimaginable.

With this statement, Palantir was dropped as a candidate for pCloudBw, the next-generation defense cloud project pursued by the Bundeswehr. pCloudBw is an initiative aimed at consolidating operational data and artificial intelligence processing capabilities scattered across military units onto a single classified cloud, and Palantir had been among the candidates under consideration prior to its removal.

Behind this exclusion lay concerns related to the North Atlantic Treaty Organization (NATO). In March 2025, NATO signed a short-term contract with Palantir to integrate the Maven Smart System into its command structure. Maven is a program that processes satellite imagery data and recommends targeting priorities. However, the routine operation and management of this program are handled not by military personnel, but by private technical staff from Palantir. German defense authorities determined that a structure entrusting management authority over tactical intelligence to a private corporation of an allied nation could undermine national defense sovereignty. The US CLOUD Act presented an additional obstacle.

This law opens the door for US law enforcement authorities to access information handled by US corporations, regardless of server location. The Ministry of Defense deemed it unacceptable for the Bundeswehr's operational plans to fall within the reach of this legislation.

Following the exclusion, the Bundeswehr sought replacement candidates within Europe. Around April 29, 2026, when Vice Admiral Daum's remarks became public, the Bundeswehr was already broadly evaluating the cloud and artificial intelligence system Altra from German company Helsing, the sovereign cloud system S3NS from German

company SAP, and the BullSequana XH3000 from French company Atos. Altra was already deployed in some Bundeswehr units, while S3NS was a system defense contractor Thales had been using to migrate its financial and procurement operations. After this broad review, the finalists for the pCloudBw project were narrowed down to three contenders.

Stuttgart-based Almato, a subsidiary of German company DATAGROUP, holds certification for processing data at the VS-NfD classification level required by Germany's Federal Office for Information Security (BSI). Berlin startup Orcrist Technologies presented technology that weaves large-scale information in varying formats into a single situational awareness display. Paris-based ChapsVision also entered the competition, led by ArgonOS. The three companies underwent tests integrating operational data during the summer of 2026, with the final winning bidder scheduled to be announced at the end of 2026.

The removal of Palantir and the selection of its replacement thus remain separate issues.

Palantir CEO Alex Karp reacted immediately to the decision. In an interview with the German media outlet Bild, he stated he was surprised by the news and likened Germany's debate to a story about magic. Karp argued that Palantir's technology had already been proven on the battlefield in Ukraine, referencing the personal ties he and co-founder Peter Thiel have shared with Germany. In response, German Digital Minister Karsten Wildberger countered that independence—not being subject to the unilateral control of a foreign corporation—is the paramount condition to safeguard in national security.

Judicial rulings also played a role in Germany becoming more cautious toward Palantir. The state of Hesse purchased Palantir's Gotham in 2017 and operated it under the name hessenDATA. On February 16, 2023, the Federal Constitutional Court of Germany ruled unconstitutional the statutory provisions that Hesse and the state of Hamburg used as legal grounds for this system in predictive policing. The court determined that extensively analyzing citizens' communication records and personal data without explicit legal authorization violates the right to informational self-determination. This ruling subsequently prompted German states to reexamine their Palantir-based systems.

However, not all states moved in the same direction. On March 20, 2025, the Ministry of the Interior of Baden-Württemberg signed a contract to introduce Palantir's Gotham program without prior consultation with the Green Party. This contract did not include a clause allowing for early termination and stipulated paying a total of 25 million euros

over five years, or approximately 9.25 million euros annually. Within the Green Party, which participated in the state coalition government, 92 percent voted in favor of immediately halting this contract. However, a contract without an exit clause could not be overturned by political opposition alone, and the state government continued with the contract.

This case demonstrates that if a state does not include termination conditions in procurement contracts in advance, the state loses its own bargaining power.

There is a point to clarify here. The European Union's Artificial Intelligence Act (AI Act) excludes artificial intelligence systems used for military, defense, and national security purposes from its scope of application. Article 2 and Recital 24 of this law ground this exclusion in the national security responsibilities borne by each member state and the nature of military activities. In other words, the decision by Germany's Federal Office for the Protection of the Constitution (BfV) and the Federal Armed Forces (Bundeswehr) to exclude Palantir was not the result of following EU-level AI regulations, but a choice made independently by Germany as an individual nation within the domains of procurement and politics.

These diverging actions by federal agencies and state governments reveal that even within the same country, the speed and manner of defending sovereignty differ. While the Federal Office for the Protection of the Constitution (BfV) and the Federal Armed Forces (Bundeswehr) excluded Palantir before signing any contracts, Baden-Württemberg remains tied to a contract it had already signed.

Sources and References

1. Unknown Author, 'Digital Sovereignty: BfV Buys European Palantir Alternative', heise online, 2026, https://www.heise.de/en/news/Digital-Sovereignty-BfV-Buys-European-Palantir-Alternative-11293717.html

2. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/

3. Unknown Author, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

4. Jonas Brandstetter, 'Bundeswehr verzichtet auf Palantir', Behörden Spiegel, 2026-05-12, https://www.behoerden-spiegel.de/2026/05/12/bundeswehr-verzichtet-auf-palantir/

5. Unknown Author, 'Palantir CEO Alex Karp Critiques German Military's Rejection of Advanced Defense Technologies', SSBCrack News, 2026, https://news.ssbcrack.com/palantir-ceo-alex-karp-critiques-german-militarys-rejection-of-advanced-defense-technologies/

6. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

7. Unknown Author, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

8. Unknown Author, 'Neue Regeln für BND und Verfassungsschutz: Regierung will Geheimdienst-Befugnisse massiv ausweiten', Tagesspiegel, 2026, https://www.tagesspiegel.de/politik/neue-regeln-fur-bnd-und-verfassungsschutz-regierung-will-geheimdienst-befugnisse-massiv-ausweiten-15786692.html

9. Unknown Author, 'Geheimdienstreform: Zeitenwende für Spione', netzpolitik.org, 2026, https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/

10. Unknown Author, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/

11. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

1.3 The Dutch Ministry of Defense's Strategy for Full Replacement Within Two Years and Switzerland's Thorough Resistance Front

The Netherlands and Switzerland distanced themselves from Palantir in ways different from France and Germany. The Netherlands has been working to systematically phase out programs already in use, while Switzerland has repeatedly chosen for years not to adopt Palantir in the first place.

Discussions surrounding the Dutch Ministry of Defense ignited when investigative news outlet Follow the Money revealed that the ministry's Special Operations Command (SOCOM) was also using Palantir, and that Palantir had access to sensitive data during military operations. In earlier reporting, Follow the Money had also disclosed that the Dutch military and police had been secretly doing business with Palantir for several years. The Ministry of Defense explained that access by Palantir employees was limited to exceptional cases, that they never worked alone without supervision, and that they handled only simulated or outdated data rather than actual classified information.

However, concerns persisted that the very fact of employees of a foreign firm accessing confidential information in any form posed a direct risk to national security. State Secretary of Defense Derk Boswijk stated that in May 2026, a month before the report was published, he had already issued internal instructions to reduce the use of Palantir. Acknowledging that reliance on Palantir was worrisome, he said he had directed the ministry to seek European alternatives. Another reason the matter sparked controversy was that Palantir also provided functionality for selecting attack targets using artificial intelligence.

On June 2, 2026, State Secretary Boswijk officially announced in the House of Representatives (Tweede Kamer) that Palantir would be replaced with European alternatives as quickly as possible. While setting a two-year target for finding fully equivalent alternatives, he admitted that no European alternative at the current level existed in the field of military artificial intelligence. He also drew a line against an immediate severing of ties, noting that cutting off relations right away could create a security void, even if limited, in operational combat systems, defense logistics, and intelligence processing.

Looking at actual progress since the announcement, observers evaluate the pace as slow. The government's follow-up response to the House of Representatives contained only expressions such as "reviewing alternatives" and "reducing dependency," instead

of specific termination deadlines. There are several reasons for the slow progress. Contracts with Palantir within the Ministry of Defense were made separately by individual sub-entities, meaning there is not even a unified contract list at the government level. This means there is no way to view ongoing, planned, or completed contracts at a single glance. Additionally, the interoperability requirement that military units must use the same systems to exchange intelligence with NATO allies serves as another obstacle.

The Netherlands' Royal Marechaussee (Marechaussee), which handles border control, also uses Palantir tools in its border surveillance system, making this an issue that cannot be resolved by a decision from the Ministry of Defense alone. Outlets covering this issue share the assessment that while the political direction has been set, the concrete momentum to put it into practice remains weak.

Switzerland is a case with a different texture. Rather than scrapping programs already adopted, as in France or Germany, it is closer to a scenario where multiple government agencies repeatedly decided over several years not to adopt Palantir.

Between April and May 2020, Switzerland's Federal Office of Public Health (FOPH) filtered out Palantir, which had participated in a tender to manage COVID-19 vaccine logistics. Although specific reasons were not disclosed, the responsible division reportedly raised objections to Palantir's participation itself. That same year, Switzerland's Federal Statistical Office (FSO) declined Palantir's requests for a meeting. Switzerland's Federal Office of Information Technology and Telecommunications (FOITT) held three meetings with Palantir between 2020 and 2021 before concluding that adoption was unnecessary. In 2020, Switzerland's Federal Office for Defense Procurement (Armasuisse) disqualified Palantir from a tender for the Military Intelligence Service's information technology system.

The reason for disqualification was failure to meet mandatory requirements, and what those requirements were was not disclosed.

In October 2022, Switzerland's Money Laundering Reporting Office (MROS) received a software demonstration from Palantir, but decided against adoption, judging that doing so would risk illegality because there was no legal basis for it. This trend continued into 2024. In June 2024, Louis Mosley, Palantir's head of European operations, met directly with Swiss Chief of the Armed Forces Thomas Süssli to pitch the products at the Shangri-La Dialogue security summit in Singapore.

Noting the Swiss military's interest in applying artificial intelligence or algorithms to data, Mosley proposed conducting a live product demonstration, including an

application that measures unit operational readiness. After receiving this proposal, the Swiss Armed Forces Staff prepared an internal evaluation report and submitted it directly to Chief of the Armed Forces Süssli in early December 2024. The report raised concerns that adopting Palantir's tools could result in confidential Swiss military information being passed to the U.S. Central Intelligence Agency (CIA) and the National Security Agency (NSA), and the Swiss military ultimately dropped its adoption plans based on this report.

As rejections across five agencies accumulated over four years, refusing Palantir became established almost like an institutional culture in Switzerland. Throughout this period, Palantir actively knocked on the doors of Swiss public offices, but ultimately failed to secure a single contract. As reported on February 14, 2026, by the security news outlet Zendata, the reason Switzerland turned Palantir away was not a lack of performance. Its proprietary and opaque internal structure, foreign legal jurisdiction, and remote update methods were assessed as uncontrollable sovereignty risks.

The Swiss side judged that simply keeping data within Switzerland and inserting protective clauses in contracts was insufficient to adequately prevent this risk.

Palantir also reacted strongly to media coverage addressing this wave of rejections. In December 2024, the Swiss investigative outlet Republik published two articles suggesting that Palantir's relationship with Switzerland could be risky. Palantir filed a lawsuit against Republik, demanding the publication of twenty-three counter-statements. The Commercial Court of Zurich ordered the publication of only one of the twenty-three statements, and the damages awarded to Palantir amounted to just 9,000 Swiss francs. This ruling dealt another blow to Palantir's credibility in Switzerland.

Around the same time, new measures emerged in Spain. The Spanish Prime Minister's Office issued instructions to state-owned enterprises under the State Company for Industrial Participations (SEPI) not to enter into new contracts with Palantir, news of which was reported in the Spanish press on July 1, 2026. This measure targeted state-owned companies handling advanced telecommunications networks and military intelligence, such as telecom company Telefónica, defense company Indra, and shipbuilder Navantia. However, existing contracts were not voided. A contract worth approximately 16.5 million euros between the Spanish Armed Forces Intelligence Center (CIFAS) and Palantir remains in effect through November 2026.

The fact that blocking new contracts and terminating existing ones are different matters is equally evident in Spain's case.

Looking at the Netherlands, Switzerland, and Spain side by side reveals that Europe does not distance itself from Palantir in just one way. The Netherlands cannot easily remove software that has already permeated throughout its defense system using political will alone. Switzerland has reached a point where renewed persuasion is hardly necessary, thanks to cumulative decisions by various agencies that prevented Palantir from crossing the threshold in the first place. Spain chose to close the door on future contracts while waiting for already signed agreements to run their course until expiration.

Either way, operating a security system without relying on American technology requires preparing everything in advance, down to every single contract clause and inter-agency agreement.

Sources and References

1. Eglė Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

2. Author unknown, 'Defensie zoekt alternatief voor Palantir-software', Computable, 2026-06-03, https://www.computable.nl/2026/06/03/defensie-zoekt-alternatief-voor-palantir-software/

3. Author unknown, 'Defensie wil software Palantir "binnen twee jaar" vervangen door Europees alternatief', Nederlands Dagblad, 2026, https://www.nd.nl/nieuws/politiek/1319116/defensie-wil-software-palantir-binnen-twee-jaar-vervangen-doo

4. Author unknown, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-verkenningen

5. Follow the Money, 'Omstreden techbedrijf Palantir kan bij geheime data van Defensie', Follow the Money, 2026, https://www.ftm.nl/artikelen/omstreden-techbedrijf-palantir-kan-bij-geheime-data-van-defensie

6. Follow the Money, 'Het Nederlandse leger doet al jaren in het geheim zaken met de omstreden techreus Palantir, net als de politie', Follow the Money, 2026, https://www.ftm.nl/artikelen/het-nederlandse-leger-doet-al-jaren-in-het-geheim-zaken-met-de-omstreden-techreus-palantir-net-als-de-politie

7. Author unknown, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/

8. Republik, 'How tenaciously Palantir courted Switzerland', Republik, 2026-02-18, https://www.republik.ch/2026/02/18/how-tenaciously-palantir-courted-switzerland

9. Republik, 'Überwachungstechnologie: Wie hartnäckig Palantir die Schweiz umwarb', Republik, 2025-12-08, https://www.republik.ch/2025/12/08/wie-hartnaeckig-palantir-die-schweiz-umwarb

10. Author unknown, 'Switzerland rejects Palantir over fears of US access to military data', 20 Minuten, 2026, https://www.20min.ch/story/kontroverser-it-konzern-palantir-umwarb-den-bund-jahrelang-und-blitzte-immer-wieder-ab-103466880

11. Author unknown, 'Palantir Took a Swiss Courtroom Loss and a European Credibility Hit', Yahoo Finance, 2026, https://finance.yahoo.com/markets/stocks/articles/palantir-took-swiss-courtroom-loss-111400896.html

12. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

2.1 The Anthropic 'Fable 5' Blocking Incident and Warning to Allies

Friction between the U.S. Department of Defense and the artificial intelligence company Anthropic had been quietly building up even before 2026. Anthropic had set two bright lines for itself when providing its artificial intelligence models to government agencies. One was that its models must not be integrated into weapon systems designed to directly target and kill human beings. The other was that its models must not be used for indiscriminate, secret surveillance targeted at domestic citizens. These two conditions were extensions of the usage policy the company had declared even before entering into contracts with the government. The leadership of the Department of Defense did not accept these conditions.

They demanded complete, unconstrained access. The substance of the Defense Department's demand was that it be able to directly connect artificial intelligence models to weapons target-selection systems or link them without limitation to surveillance systems that filter the communications and location data of domestic citizens. Anthropic viewed accepting such demands as directly involving its artificial intelligence in life-or-death decisions or full-scale surveillance of domestic citizens. The company held firm in its position to maintain these two lines, even at the risk of losing a government client. The gap in negotiations could not be narrowed.[1]

When Anthropic refused to back down, the Department of Defense designated the company as a threat to the nation's software supply chain. Defense officials formally designated Anthropic as a supply chain risk enterprise critical to national security. This designation was a severe administrative measure that had previously been applied only to corporate entities based in countries hostile to the United States. It was unheard of until then for a private artificial intelligence company to receive such a designation.

On February 28, 2026, the Trump administration ordered federal agencies to cease using Anthropic's artificial intelligence programs.[1] On the surface, this order appeared to be an administrative action dealing with procurement regulations, but in practice, it served as a tool to pressure Anthropic into accepting the access terms requested by the Department of Defense. The designation of supply chain risk enterprise was not merely heavy terminology. Entities receiving this designation were classified as untrusted suppliers within the Department of Defense procurement system, making it difficult to secure new contracts and typically subjecting existing contracts to reexamination.

Until then, this measure had been used to filter out entities connected to countries hostile to the United States. Never before had a globally recognized artificial intelligence developer based in Silicon Valley been placed on this list. The fact that Anthropic received this designation demonstrated in itself that the Department of Defense was treating this conflict not as a negotiation over contract terms, but as a matter of national security threats.

Anthropic did not back down against this pressure, and the matter moved to the courtroom. On March 27, 2026, a federal judge declined to side with the Department of Defense. The judge ruled that the pressure exerted by the Department of Defense on Anthropic constituted political retaliation violating freedom of speech guaranteed under the First Amendment of the Constitution.[1] It was an incident where a private company collided head-on with public power while seeking to uphold self-imposed usage terms, a collision that culminated in a judicial ruling. Within the United States, this ruling demonstrated that checks and balances were functioning.

When the executive branch's pressure on a private company was judged unfair, the judiciary could step in to block it. However, this judicial check was effective only within the borders of the United States. Up to this point, it was a dispute between the executive branch and a private company taking place inside America, and European governments and institutions had no way to monitor the outcome of this struggle, nor any means to intervene in it.

This internal conflict did not end with domestic litigation. On June 12, 2026, the U.S. Department of Commerce issued an order restricting exports of artificial intelligence technology. The Department of Commerce cited the preservation of top-tier national security as the rationale for this action.[2][3] The explicit target of this order was access by users holding foreign nationality.[2] However, Anthropic did not possess a filtering system capable of screening the nationality of incoming connections in real time. Even if a company providing services over the internet could determine the country where an account was registered or where a payment card was issued, immediately verifying the nationality of every individual user connecting to the service was no simple task.

Consequently, Anthropic chose to completely halt overseas internet access to its highest-performing models, Claude Fable 5 and Claude Mythos 5. Within hours of the order's delivery, connections from all foreign computers, including those in Europe, were severed.[1][5] Although the government directive targeted foreign nationals, what was actually cut off was all overseas access regardless of nationality. This action differed in nature from sanctions where the United States permanently places specific companies or individuals on a trade blacklisting registry.

The mechanism deployed by the Department of Commerce was an order temporarily restricting technology exports on national security grounds, and such orders by nature could be revoked at any time based on policy judgments, even if legally issued without a predefined time limit. For European user institutions, however, understanding these legal nuances did nothing to lessen the shock of the moment access was cut off.

Numerous European government agencies and research institutes lost the artificial intelligence software they relied on daily without any prior warning.[1][5] There were no announcements explaining why access was severed, nor any channels provided to raise objections. The situation was no different for institutions that had signed contracts and paid service fees. The right to receive continued service held no weight against the export control determinations of the supplier nation's government, overriding user contracts. Cloud service terms of use and service level agreements were not mechanisms capable of shielding users against state administrative actions of this nature.

European cybersecurity publications covered the crisis under the moniker 'Fable-Ban.' The focus of their reporting was the fact that a single executive order from a friendly nation could freeze the operational networks of allied countries without any prior consultation.[5]

Government ministries were not the only ones to lose access. Administrative agencies across European nations, along with universities and national research institutes, were using Fable 5 and Mythos 5 in their daily operations, and these entities lost their tools at the exact same moment in the exact same manner.[8] This disruption, experienced jointly by both the public and academic research sectors, served to broaden awareness that the crisis was not an issue confined to a specific ministry or contract, but a problem spanning all European users dependent on American technology.[8] In an article titled on how American software could be weaponized, the German cybersecurity publication SecureCloud Blog examined the controversy surrounding Palantir alongside the Fable 5 ban, concluding that what Europe needed was not distrust of individual companies, but digital sovereignty.[5] The article pointed out that regardless of which company a contract was signed with, it remained difficult to fully escape the same risk as long as that company was headquartered in the United States.[5]

This block lasted for 18 days. The U.S. government lifted export restriction measures only on July 1, 2026.[3] Anthropic stated that it began the process of restoring access after controls were lifted.[4] According to the company's explanation, access severed by the June 12 action was not restored completely and immediately upon the lifting of controls, but rather proceeded as a gradual recovery.[4] A reversal in policy did not

mean the service turned back on at that exact moment. Reestablishing severed connections also took time. The block had taken effect just hours after the order was delivered, but restoration was not as fast.

More time was required to return completely to the previous state. Nevertheless, the outcome of the incident was clear: access was severed, and then it was reopened.

Two facts need to be confirmed here. First, overseas access to Fable 5 and Mythos 5 was indeed cut off. Numerous European government agencies and research institutes had to work without these tools for 18 days. Second, the block did not last permanently. The U.S. government changed its policy, and access reopened. Reading this incident as proof that American artificial intelligence technology will never again be supplied to Europe is factually incorrect. Anthropic continued operating in Europe after the incident, and European institutions also renewed contracts or maintained existing agreements.

Conversely, brushing off this incident as if nothing had happened is also factually incorrect. While the disruption that actually occurred over those 18 days did not leave irreversible losses, institutions requiring access during those 18 days had no choice but to find alternatives or postpone their work. What the Fable 5 incident actually demonstrated was a structure in which supply could stop at any time, and the authority to decide that stoppage and resumption rested not with the user country, but with the home government of the supplying company. The conflict that triggered this incident was not aimed at Europe from the beginning.

The dispute between the Department of Defense and Anthropic was an extension of procurement negotiations taking place within the United States, and Europe had nothing to do with those negotiations. Nevertheless, European governments and research institutes bore the consequences of those negotiations together. The fact that work tools could be cut off in the aftermath of a dispute unrelated to themselves left even greater anxiety than if they had been a party to the conflict. European governments and institutions had no way of predicting what trigger might sever access in the same way next time.

Until then, this structure had been an intangible concept to European policymakers. The term digital sovereignty was an expression that appeared only in presentations at academic seminars or in the prefaces of policy reports.[1] The fact that a single export control order issued by an allied government while resolving its own domestic political dispute could suspend the work tools of allied government agencies within hours became an actual occurrence rather than mere theory.[1][5] Although the target of the Department of Commerce's order was foreign nationals, the resulting casualty was the access of allied governments and research institutes.

This mismatch between target and result was the reason Europe took this incident as a grave warning. Even though the United States had not targeted Europe with its measures, the very fact that Europe fell within the range of those measures was the problem. U.S. export controls were typically a tool used to prevent technology leakage to hostile nations, and friendly nations, including North Atlantic Treaty Organization (NATO) member states, had customarily been set apart from such targets. However, in the Fable 5 incident, this distinction was not maintained in practice.

The boundary separating allies from non-allies existed only within policy intent and was not supported by technical mechanisms to filter by nationality. What European governments read from this incident was precisely this gap: the fact that the gulf between intended distinction and practical enforcement could not be bridged by allied status alone.

The country that moved fastest was France. On June 16, 2026, four days after the Department of Commerce's export control order was issued, French Interior Minister Sébastien Lecornu announced that the intelligence analysis system of France's General Directorate for Internal Security (DGSI) would be switched from American company Palantir's program to ArgonOS, developed by French company Hapsvision.[6] This announcement should not be read as meaning that the contract with Palantir ended on the spot. The contract between Palantir and the French government still had several years remaining at that point, and terminating the contract would require penalty payments and separate negotiations.

The actual system replacement was also a separate process that unfolded after the announcement.[7] Nevertheless, the fact that the French government issued an announcement in this direction just four days after the Department of Commerce's order demonstrates how quickly the Fable 5 block transitioned into policy discussions within European governments. France was merely the first country to issue an announcement in this shift, not the only one.

In the months following the Fable 5 block, procedures to reexamine reliance on American technology began in succession across other European governments.[8] Although the specific path taken by each nation varied, the fact that this incident served as the starting point was common to all.

The lesson Anthropic's case left for Europe was not that a single company could not be trusted. Anthropic upheld its own terms of service against the demands of the Department of Defense, and the court ruled in the company's favor. The pressure the company endured while maintaining its two lines against lethal weapons and indiscriminate surveillance demonstrated, if anything, that it remained faithful to its

established principles. What was identified as the problem was not Anthropic's stance, but the structure itself, in which the U.S. government could halt the overseas services of any American firm in the exact same manner whenever it decided to do so.

Today it was a conflict between the Department of Defense and Anthropic, but next time a different conflict with a different company could produce the same outcome. This held true whether the conflict stemmed from a trade dispute, security policy, or internal negotiations between government and business as in this case. European governments and research institutes found themselves on the receiving end of the consequences despite not being parties to the dispute.

Eighteen days was not a short period for actual operations to come to a halt. At the same time, the incident confirmed that such a period would eventually come to an end. Once the U.S. government's judgment shifted, access reopened. This was precisely why multiple European governments began reexamining their national technology procurement policies after the incident. The incident made clear that no matter how detailed the provisions in a contract might be, those clauses held no power against a decision by the vendor's home government. More lingering than the fact that access had been severed was the reality that the authority to determine its start and end lay beyond their own hands.

The Fable 5 incident was thus recorded in European policy documents not as a story of a block that lasted forever, but as a reminder that a block could happen again at any time and that the authority to make that decision rested with another country's government. This is why the incident continues to be cited even after access was restored. The question that remained after the crisis passed was not what had been cut off, but whether another country's government could make the same decision next time. As long as Europe cannot control the answer to this question, the 18-day block remains not a one-off accident, but a possibility that could recur.

References and Bibliography

1. Centre for Future Generations, 'Enforcement spotlight, Spring 2026', Centre for Future Generations, Spring 2026 issue.

2. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, June 12, 2026, https://www.anthropic.com/news/fable-mythos-access

3. Gyana Swain, 'US reverses export restrictions on Anthropic's Fable 5, Mythos 5 AI models', Computerworld, July 1, 2026, https://www.computerworld.com/profile/gyana-swain-2/

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, https://www.anthropic.com/news/redeploying-fable-5

5. Sebastian Deck, 'US Software as a Weapon: Palantir's Manifesto Dramatically Highlights the Need for Digital Sovereignty', SecureCloud Blog, June 8, 2026, https://blog.securecloud.de/en/us-software-als-waffe-palantirs-manifest-zeigt-drastisch-notwendigkeit-digitaler-souveraenitaet

6. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, June 16, 2026, https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision

7. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, June 17, 2026, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

8. 'Analysis Report on Major European Union (EU) Countries' Move Away from Palantir and Digital Sovereignty' (Yuropeon-yeonhap (EU) Juyo-guk-ui Tal-Palantier Haengbo-wa Dijiteol Jugwonhwa-e Gwanhan Bunseok Bogoseo), 2026, pp. 1-2.

2.2 The Trap of Extraterritorial Legislation: The Reality of Judicial Reach Under the U.S. CLOUD Act and FISA Section 702

Member states of the European Union have long believed that keeping data servers within their national territories ensures the safety of their information. American companies like Amazon, Microsoft, and Google built data centers in Frankfurt, Paris, and Dublin, using this belief as a promotional tagline. However, the fact that a server stands on European soil and the fact that the information inside that server remains beyond the reach of U.S. law are two different matters. This is because two statutes enacted by the U.S. Congress—the CLOUD Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA)—operate based on corporate affiliation rather than national borders.

To understand why these two laws are currently putting European procurement officials on edge, one must first look at the background behind the birth of the CLOUD Act. In December 2013, U.S. federal law enforcement agencies served Microsoft with a warrant demanding the surrender of a user's email account information in connection with a drug trafficking investigation. The issue was that the account's data was stored on a server in Dublin, Ireland. Microsoft filed a lawsuit arguing that a U.S. warrant does not extend to data outside U.S. territory, and in 2016, the U.S. Court of Appeals for the Second Circuit in New York ruled in Microsoft's favor.

While the U.S. Department of Justice appealed this ruling to the Supreme Court, the U.S. Congress passed the CLOUD Act on March 23, 2018. Because the new law altered the very legal foundation of the dispute, the Supreme Court determined there was no need for further review and dismissed the case. The CLOUD Act was thus born out of an effort to resolve through legislation a legal battle that the U.S. government was on the verge of losing in court.

The core of the law is simple. It does not ask in which country the data is stored. It asks whether the company managing that data falls under U.S. jurisdiction. In legal terms, this is expressed through three criteria: possession, custody, or control. If a company is headquartered in the United States or is an overseas subsidiary where a U.S. firm holds equity and managerial control, any information possessed, kept, or controlled by that company must be submitted pursuant to a warrant or order from a U.S. court, regardless of its physical storage location.

At this point, it is necessary to distinguish between what the CLOUD Act actually enables and what people frequently misunderstand. What the CLOUD Act enables is clear: telecommunications service providers or remote computing service providers subject to U.S. jurisdiction bear a legal obligation to comply with lawful U.S. government demands to produce information they possess, keep, or control, regardless of which country's servers hold that information. On the other hand, there are several things the CLOUD Act does not automatically imply. First, this law does not mean the U.S. government already has all data in its hands.

The government must still go through formal legal procedures for each individual case, such as obtaining a court warrant or a prosecutorial subpoena. Second, it does not mean that every demand is automatically enforced. The CLOUD Act opens only a narrow channel for companies to challenge requests in court, restricted strictly to citizens of foreign governments that have entered into a formal executive agreement with the U.S. government. As of 2022, the United Kingdom and Australia are the only two countries that have concluded such agreements, and the European Union has yet to sign one with the United States. Therefore, for information belonging to European citizens, even this exceptional challenge procedure does not apply.

Even in the case of the United Kingdom, which has signed an agreement, this channel is narrow. Courts will accept a challenge only if the target of the request is not a U.S. citizen and does not reside in the United States, and the company must prove that handing over the information actually conflicts with U.K. law. In cases like the European Union where no agreement exists at all, even this limited channel is nonexistent. Third, the scope of this law depends on corporate nationality and governance structure, not on the physical location of the servers. A purely European company with no equity or managerial ties to the United States is not subject to the CLOUD Act.

It is easy to understand this mechanism by tracing it through a concrete scenario. Suppose an administrative ministry in France enters into a contract with a U.S. company's European subsidiary, including a clause stipulating that data must remain strictly within French territory. This contract is an agreement between the French government and the European subsidiary. However, if U.S. prosecutors want that data, they do not serve a warrant on the subsidiary in France; they serve it on the parent company in the United States. Because the parent entity holds equity and management control over the subsidiary, it is legally deemed to be in possession, custody, or control of that data.

When the parent company instructs the subsidiary to submit the data, the subsidiary has no choice but to comply with that directive, regardless of its contract with the French government. The French government was merely a party to the contract and has no authority to intervene in this internal corporate direction process. Even if the data never leaves French territory once, this procedure unfolds in exactly the same way. This is why the condition of data remaining in Europe does not eliminate legal risk. What determines the risk is not the physical location of the server, but the nationality and governance structure of the company managing that server.

Another layer compounds this situation. Article 48 of the European Union's General Data Protection Regulation (GDPR) stipulates that even if a foreign court or administrative authority demands the transfer of personal data, that demand cannot be recognized or enforced within Europe unless it is based on an international agreement concluded with the European Union or its member states. However, as noted earlier, no bilateral executive agreement under the CLOUD Act exists between the United States and the European Union. Ultimately, a company served with a U.S. warrant is trapped between two conflicting laws.

If it complies with the U.S. warrant, it hands over information without the international agreement basis required by EU law; if it refuses the warrant, it faces contempt of court charges in a U.S. court. This conflict is not a theoretical paper debate, but a structural dilemma that American cloud companies face every time they contract with European clients.

The case of Italy illustrates how deep-rooted this dilemma is. When the Italian government established the Polo Strategico Nazionale, its sovereign strategic cloud for public administration, it designed the system to keep data strictly within Italian territory and mandated that its own government agency directly manage the encryption keys. However, the underlying technology actually powering this strategic cloud came from American hyperscalers like Microsoft Azure and Google Cloud. Even holding the keys in hand, Italian authorities could not completely erase the fundamental limitation that the lock mechanism itself locked by those keys was designed and supplied by American companies.

Even after erecting two layers of defense—data localization and encryption keys—the third layer, the nationality of the core software technology, remained firmly with the United States.

This reality was confirmed not through abstract statutory text, but through actual testimony. On July 17, 2025, an executive in charge of legal affairs at Microsoft testified under oath before a hearing of the French Senate. He admitted that even for user data

physically stored in Paris, if U.S. federal law enforcement agencies demand the surrender of information based on the CLOUD Act, the company has no choice but to hand over that information without the approval of the French government.

When the American business magazine Forbes reported this testimony on July 22, 2025, procurement officials across Europe received documented confirmation of the fact that hosting servers on their own territory alone could not place them beyond the reach of U.S. law.

Paired with the CLOUD Act, another threat is Section 702 of the Foreign Intelligence Surveillance Act (FISA). Included in the FISA Amendments Act enacted in 2008, this provision allows intelligence agencies such as the U.S. National Security Agency (NSA) to collect communications records and internet data of foreigners outside U.S. territory without obtaining individual court warrant reviews for each target. Where the CLOUD Act is a law enforcement tool triggered by specific requests from investigative agencies, Section 702 is a broad surveillance authority exercised by intelligence agencies under the mantle of foreign intelligence gathering. Because it is a temporary provision with a sunset clause, the U.S. Congress must revisit and reauthorize it every few years.

In April 2024, the U.S. Congress extended Section 702 through the Reforming Intelligence and Securing America Act, setting its expiration date for April 2026. Congress later pushed the deadline back once more to June 12, and when new reauthorization legislation failed to pass by that point, the statutory text itself lapsed at midnight on June 12, 2026. However, one-year surveillance certifications already approved by the U.S. Foreign Intelligence Surveillance Court in March 2026 were designed to remain valid even after the statute expired, leaving actual surveillance powers fully operational through March 2027.

This disconnect between the legal status of the statute and the continuation of actual surveillance demonstrates how difficult it is to control this authority through a single law. Numerous reports have pointed out that this surveillance network captures not only ordinary citizens, but also the email transmission routes of generals and senior diplomats from allied nations. How Section 702 actually operates was revealed in detail in 2013 through disclosures by former U.S. intelligence contractor Edward Snowden.

According to documents disclosed at the time, the U.S. National Security Agency relied on this provision to run a collection system called PRISM, obtaining foreign users' data directly from the servers of American companies like Google, Microsoft, and Yahoo. These disclosures prompted European governments to recognize Section 702 not as a paper statute, but as a functioning, active surveillance infrastructure.

The case in which this surveillance structure first collided head-on in a European courtroom was the Schrems ruling. On July 16, 2020, in a lawsuit brought by Austrian citizen Maximilian Schrems, the Court of Justice of the European Union ruled that U.S. surveillance systems severely infringed upon European citizens' right to informational self-determination, invalidating Privacy Shield, the data transfer agreement between the United States and the European Union. What the court took issue with was nothing other than America's warrantless surveillance powers such as Section 702.

The crux of the ruling was that no matter how meticulously European companies drafted data protection clauses into their contracts, as long as that information traversed the networks of U.S. corporations, private agreements could not block the surveillance authority of U.S. intelligence agencies. The European Commission also explicitly identified both the CLOUD Act and Section 702 as structural security defects inherent in Europe's digital territory in an impact assessment for the Cloud and AI Development Act proposed on June 3, 2026.

This issue extended beyond statutory interpretation to actively reshape practical procurement policies. The Ministry of the Interior of the German state of Baden-Württemberg conducted a detailed analysis of the operational conditions of Delos Cloud, a public cloud initiative built on Microsoft software. The conclusions were unambiguous: while the data centers themselves were certified by Germany's Federal Office for Information Security (BSI) and operated within German territory, control over the design and management of the application software running on top of them still belonged to Microsoft in the United States.

The state ministry concluded that as long as control over the application layer rested with an American corporation, one could not rule out the possibility that U.S. security agencies might instruct the software provider to covertly embed data exfiltration channels without users' knowledge. The physical presence of data inside Germany did not eliminate this risk.

Similar concerns translated into official policy action in the Netherlands. In November 2025, U.S. IT enterprise Kyndryl announced plans to acquire Dutch firm Solvinity. Solvinity was the company operating the underlying infrastructure for DigiD, the digital identity system used by roughly 16.5 million Dutch citizens. Concerns grew in the Dutch House of Representatives that the takeover could open a channel for U.S. legal jurisdiction to access citizens' sensitive identity information, leading the government to initiate steps to block the transaction.

On May 26, 2026, State Secretary Aartsen of the Dutch Ministry of Economic Affairs announced that the government was formally blocking Kyndryl's acquisition of

Solvinity on grounds of protecting the public interest. The reasoning stated by the government was clear: U.S. law theoretically permits American authorities to obtain data stored on the servers of foreign subsidiaries owned by U.S. parent companies. This was the first time that the Dutch Investment Screening Bureau, established in 2020, had blocked an acquisition by an American firm. The Center for Strategic and International Studies (CSIS), a U.S. think tank, described the decision as a bellwether for how investment screening criteria across European nations will evolve.

In the United Kingdom, the issue manifested as contracts themselves handing state secrets over to U.S. companies, regardless of physical location. American data analytics firm Palantir entered into a £15 million cloud support contract with the Atomic Weapons Establishment (AWE), Britain's nuclear weapons research facility. According to investigative outlet The Nerve, which reported on the contract in January 2026, the agreement was omitted from the government's official public procurement portal, and the Ministry of Defence neither confirmed nor denied the contract's existence.

The same report calculated that Palantir's total contracts with the UK government reached £670 million, with the deal involving the nuclear facility remaining undisclosed on the public roster. The House of Commons Science and Technology Committee pointed out that the existing architecture—relying on American companies for national law enforcement surveillance networks and public health data—represented a severe vulnerability in the procurement system. The omission of a contract handling nuclear weapons data from public procurement registries served as a stark reminder that signing agreements within physical borders does not ensure that control over information remains in home hands.

In Germany, another legal clash involving Palantir took place, though it is important to distinguish that this case turned on the German Constitution rather than the CLOUD Act or Section 702. On February 16, 2023, Germany's Federal Constitutional Court ruled that the police use of software to run predictive analytics on citizens unsuspected of any crime was unconstitutional. The Hessendata system struck down by the court was a policing platform built on Palantir's Gotham software. What this ruling challenged was not the extraterritorial reach of U.S. law, but the right of citizens to informational self-determination protected under Germany's Basic Law.

Although these two issues stemmed from different root causes, they ultimately pointed to the same conclusion: an architecture that entrusts national policing and security data to American corporate software can be destabilized from multiple directions at once—whether by U.S. statutes or domestic constitutional mandates.

It was confirmed that U.S. extraterritorial jurisdiction can be used not only to demand information but also as a tool for sanctions. On August 20, 2025, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on International Criminal Court judges involved in issuing an arrest warrant for Israeli Prime Minister Netanyahu. French judge Nicolas Guillou was among those targeted. He later told the press that his bank card payments and access to Amazon services had been blocked. Reports also surfaced that the email account of another sanctioned International Criminal Court official had been suspended by Microsoft, though Microsoft denied the claim.

Although this incident rests on sanctions regulations distinct from the CLOUD Act or Section 702, it demonstrates the exact same underlying risk. Individuals and institutions that rely on payment, communications, and cloud services provided by U.S. companies can lose access to everyday services all at once through a single decision by the U.S. executive branch.

France embedded this requirement directly into the explicit language of its certification standards. In revising the SecNumCloud certification criteria granted to trusted cloud providers, France's National Agency for the Security of Information Systems (ANSSI) explicitly stated that keeping data inside Europe is not enough. The SecNumCloud 3.2 standard, updated in 2025, added a new requirement for providers seeking certification: in addition to locating their headquarters and data centers within the European Union, a company's capital and voting structures must remain completely independent from third-country laws with extraterritorial effect, such as the CLOUD Act.

This means that to earn certification, a provider must establish a framework where data disclosure orders from third countries, issued without going through international mutual legal assistance procedures, cannot take effect. The fact that French authorities effectively singled out the CLOUD Act in the text of the certification criteria demonstrates that European policymakers defined this issue not as a matter of contractual trust clauses, but as a problem that must be solved through corporate ownership structures.

Placing these various cases side by side reveals a single conclusion. Policies keeping data within European territory are necessary, but they are not sufficient on their own. To genuinely reduce risk, the company handling the information must itself be free from U.S. ownership, control, and software design authority. A server's location is merely a coordinate on a map, whereas the authority to actually open or close access to the information at those coordinates depends on which country's laws govern the

company's headquarters. This is precisely why European governments are expanding their scope of review from physical data sovereignty to corporate governance structures and core software technology.

The European Commission translated this distinction into policy language in its impact assessment for the Cloud and AI Development Act. The assessment evaluated three separate layers: the physical storage location of data, the entity managing the encryption keys, and the ownership structure of the company designing and supporting the software. France's SecNumCloud certification addressing corporate capital structure, and Italy's Strategic Cloud failing to declare full independence even while holding the encryption keys, are examples proving in their own ways that practical protection exists only when these three layers are established together rather than functioning in isolation.

References and Sources

1. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943 (Public Law 115-141), March 23, 2018. https://www.congress.gov/bill/115th-congress/house-bill/4943/text

2. U.S. Congress, Foreign Intelligence Surveillance Act Amendments Act of 2008, Section 702 (Public Law 110-261), 2008.

3. U.S. Congress, Reforming Intelligence and Securing America Act (RISAA), April 20, 2024. https://www.congress.gov/crs-product/R48592

4. Electronic Frontier Foundation, 'Victory! 702 has Expired!', EFF Deeplinks, June 2026. https://www.eff.org/deeplinks/2026/06/victory-702-has-expired

5. Court of Justice of the European Union, 'Maximillian Schrems v. Facebook Ireland Limited', Case C-311/18, judgment of July 16, 2020.

6. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 48.

7. Polo Strategico Nazionale, 'Secure Public Cloud: the encrypted cloud', polostrategiconazionale.it. https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/secure-public-cloud/

8. United States v. Microsoft Corp., 584 U.S. ___ (2018), Supreme Court of the United States. https://supreme.justia.com/cases/federal/us/584/17-2/

9. Emma Woollacott, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, July 22, 2025. https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

10. European Commission, Impact Assessment accompanying the proposal for the Cloud and AI Development Act, SWD(2026) 502 final, June 3, 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

11. Center for Strategic and International Studies, 'Untapping the Full Potential of CLOUD Act Agreements', CSIS Analysis. https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements

12. netzpolitik.org, 'Delos-Cloud: Mit Microsoft in die digitale Abhängigkeit', netzpolitik.org, 2024. https://netzpolitik.org/2024/delos-cloud-mit-microsoft-in-die-digitale-abhaengigkeit/

13. NL Times, 'Netherlands blocks U.S. takeover of DigiD operator Solvinity over security concerns', NL Times, May 26, 2026. https://nltimes.nl/2026/05/26/netherlands-blocks-us-takeover-digid-operator-solvinity-security-concerns

14. Cleary Antitrust Watch, 'Dutch Government Blocks Kyndryl's Acquisition of Solvinity in First-Ever Telecom FDI Prohibition', Cleary Antitrust Watch, June 2026. https://www.clearyantitrustwatch.com/2026/06/dutch-government-blocks-kyndryls-acquisition-of-solvinity-in-first-ever-telecom-fdi-prohibition/

15. The Nerve, 'Revealed: Palantir deals with UK government amount to at least £670m – including £15m contract with nuclear weapons agency', The Nerve, January 2026. https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley

16. Bundesverfassungsgericht, Judgment on the HessenDATA predictive policing program, February 16, 2023.

17. Irish Times, ''It's surreal': US sanctions lock International Criminal Court judge out of daily life', Irish Times, December 12, 2025. https://www.irishtimes.com/world/us/2025/12/12/its-surreal-us-sanctions-lock-international-criminal-court-judge-out-of-daily-life/

18. Computer Weekly, 'Microsoft's ICC email block reignites European data sovereignty concerns', Computer Weekly, 2026. https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns

19. cio-online.com, 'SecNumCloud, une protection contre le droit extraterritorial, pas une garantie absolue', CIO Online, 2025. https://www.cio-online.com/actualites/lire-secnumcloud-une-protection-contre-le-droit-extraterritorial-pas-une-garantie-absolue-16759.html

20. LSTI, 'SecNumCloud Qualification (ANSSI): Audit & Evaluation', LSTI Certification. https://www.lsti-certification.fr/en/Company-offers/Cybersecurity/SecNumCloud

21. Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', The Washington Post, June 6, 2013.

22. Center for Strategic and International Studies, 'The Kyndryl-Solvinity Case: A Barometer for Investment Security Reviews?', CSIS Analysis, 2026. https://www.csis.org/analysis/kyndryl-solvinity-case-barometer-investment-security-reviews

2.3 'Air-Gap' and Independent Architecture: Technical Isolation Beyond Contractual Clauses

Microsoft's head of legal affairs testified under oath at a French Senate hearing in July 2025. He stated that even if user data is stored in Paris, if a U.S. federal investigative agency demands information under the CLOUD Act, the company has no choice but to hand over the materials even without the approval of the French government. This testimony made one fact clear to European administrative officials: keeping data within national borders and filling contracts with security clauses are not enough to escape the reach of U.S. judicial jurisdiction.

A contract is originally a written record of promises agreed upon by transacting parties. Various European governments have also signed contracts with American cloud companies, inserting clauses stating that data will not be moved offshore and that information will not be handed over without an order from a European court. However, such clauses hold power only in situations where the contracting company is free to keep those promises. As long as that company is subject to U.S. law, if the U.S. government orders the submission of information based on domestic law, the company must choose between its contractual promises and its home country's laws, and in most cases, it has no choice but to obey its home country's laws.

The moment a corporate partner is forced to choose between an order from its own government and a contractual promise, the wording of the contract is no longer a shield.

This fact shattered a safeguard that European countries had relied on for a long time. European Union privacy regulations have long required data to be stored within the region, and many public institutions have believed that information is safe as long as servers remain inside national borders. This requirement is called data localization. However, data localization only specifies which country the information physically resides in; it does not specify who designed the software processing that information or who holds remote access authorization. Server location and system control are two separate issues.

An analysis by the Ministry of the Interior of the German state of Baden-Württemberg made this difference concrete. The Delos Cloud project examined by the state government was designed to store data physically on servers within German territory. However, the authority to design and update the application running this cloud remained in the hands of Microsoft's U.S. headquarters. Based on this fact, the state

interior ministry concluded that even if data resides on German soil, as long as control of the system remains in the hands of an American company, it cannot step out of the reach of search warrants under the CLOUD Act.

The issue was not where data was stored, but who designed the software handling that data and who issued update commands.

ArgonOS, selected by France as the intelligence system for France's General Directorate for Internal Security (DGSI), responds to the problems exposed by these two cases in a different way. Hapsvision, the developer of ArgonOS, is a company fully owned by European shareholders. The system operates only in air-gapped environments completely cut off from external wired networks, or on sovereign cloud servers blocked from external access. If the company that owns the system has no U.S. corporate entity and the network hosting the system has no channels reaching outward, even if U.S. judicial authorities issue a warrant, no physical or digital pathway exists to execute that warrant.

In this way, network architecture and ownership structure create isolation, rather than promises written in a contract.

There is one more aspect to this isolation that goes beyond measures protecting data itself. ArgonOS was designed to independently manage the life cycle of encryption keys that lock data while processing tens of thousands of heterogeneous structured and unstructured data items. Even if data is encrypted, if an outside company manages the key, the party holding the key can open the lock at any time. Keeping encryption key management completely separate from external access means locking not only the contents of the data but also the authorization to read that data inside the host country.

Isolation actually works only when both server location and decryption authority are secured together.

The term air-gap literally refers to keeping a physical gap between a computer network and the outside internet. Because no cables are connected, there is no way to issue remote disconnection commands or forcibly shut down the system. The Fable 5 block incident in June 2026 was a case targeting precisely this point. Anthropic's model was delivered over the internet, and overseas access was suspended entirely within hours by a single order from the U.S. Department of Commerce. A service that relies on external networks, no matter how thorough its contract, is helpless before an administrative order from the country where the provider's headquarters is located.

Conversely, for a system with no external connectivity channels to begin with, no physical path exists to transmit such an order.

However, adopting an air-gapped architecture does not immediately deliver complete security. The French Ministry of the Interior stated that it would take 18 to 24 months for France's General Directorate for Internal Security (DGSI) to migrate its entire operational intelligence activities to ArgonOS. Agents who have grown accustomed to Palantir's interface over decades must readapt to the new system, and because existing accumulated data storage standards were designed for U.S. systems, risks remain that information might be lost or formatting corrupted during migration. To bridge this gap, the French state administration promised a transition period through 2027 during which the old and new systems will run side by side.

A gap of several years separates the decision to move to an isolated architecture from the point when that architecture becomes fully operational, and during those years, the burden of maintaining two separate systems at the same time falls squarely on the intelligence agency.

The costs incurred during this gap extend beyond the migration period itself. A system severed from external networks is also cut off from real-time updates and threat-intelligence sharing services provided by major cloud companies. Agencies operating an independent system like ArgonOS must handle security patches and feature upgrades using their own workforce, a choice that also means giving up the economies of scale automatically provided by the global data center networks of major U.S. cloud providers.

In an environment without any external channels, even software updates cannot be handled through automated online distribution, often requiring physical transfer using verified storage devices. Such procedures are slower than online updates and demand dedicated verification personnel to check update contents every single time. This is why European decision-makers do not present isolation as a panacea even while choosing it. Isolation protects against the threat of a foreign government's unilateral order shutting down a system, but in return, the nation itself must shoulder the burden of ongoing maintenance.

The criterion distinguishing the problems an air gap can solve from those it cannot also lies in how much computing power a system requires. A system responsible for an agency's intelligence analysis, such as ArgonOS, can operate in a fully isolated environment even with a relatively limited number of servers. However, the situation is different for large-scale artificial intelligence models like Fable 5, which constantly demand massive amounts of computation. Training and running such models within national territory while disconnected from the outside world requires data centers, electricity, and semiconductors on a scale that no single agency can manage on its own.

This is why the challenge left to Europe by the Fable 5 blocking incident expanded beyond air-gapping individual systems to the task of building continent-scale computing infrastructure.

The responses of Switzerland and the Netherlands show that there is more than one path to achieving isolation. Swiss federal agencies rejected Palantir's bids at least nine times between 2018 and 2025, keeping the company's systems out from the beginning. Unlike France or Germany, which are removing already adopted systems and migrating to new architectures, Switzerland avoided the costly process of migration altogether. In June 2026, the Netherlands Ministry of Defence submitted a roadmap to parliament to replace Palantir within two years, but that roadmap remains a plan, and the point at which the old system is actually shut down and the new system becomes fully operational lies further in the future.

The choice to avoid creating dependency from the outset and the choice to dismantle an existing dependency may head toward the same destination, but they incur very different costs.

Even a state of completed isolation is not permanently fixed. When American company Kyndryl announced its acquisition of Solvinity, a local Dutch firm supplying core software for the Netherlands' administrative network, the Dutch House of Representatives expressed grave concern that ownership of infrastructure handling data on 16.5 million citizens could transfer to an American company overnight. Even if a system is owned by a European company today, should that company be acquired by foreign capital tomorrow, isolation contingent on ownership structure collapses instantly.

This is why the process of verifying isolation cannot stop at a one-time audit at the moment of adoption, but must extend to procedures that continuously monitor changes in ownership and governance structures.

Friction created by isolated architecture also emerges in cross-border military cooperation. On June 22, 2026, after the NATO Security Accreditation Board certified Palantir's Maven Smart System for full weaponized operations, supreme NATO commanders criticized individual member states' anti-Palantir measures in law enforcement and administration as decisions that degrade military battlefield efficiency. The choice to move domestic law enforcement intelligence networks to the air-gapped ArgonOS collides within the same country against the reality that the targeting intelligence network shared by allied forces still runs on Palantir software.

Even if a nation's intelligence agency completes isolation within its own territory, it cannot isolate the intelligence network of the entire alliance to which that nation belongs. Where to draw the boundary of isolation is a technical question as well as a political choice defining how to maintain allied relations.

A gap also remains between a political declaration and the completion of an architecture. Even after Minister Lecornu announced the transition to ArgonOS, Palantir stated that its existing contract with France's General Directorate for Internal Security (DGSI) remained legally valid. A government announcement, the shifting of procurement procedures, the actual termination of a contract, and the full replacement of a system do not happen simultaneously on a single day. Between the moment a political declaration is made and the moment the old system is actually powered down lies a separate process of negotiation and implementation, during which the old contract may remain alive on paper.

An announcement to terminate a contract does not itself complete isolation; proof of completion lies not in a press release, but in the old system actually ceasing operation and the new system actually commencing operation.

These decisions by France and Germany are also noteworthy because individual governments made them without waiting for European Union-wide laws to be enacted. The transition of France's General Directorate for Internal Security (DGSI) to ArgonOS and the same choice by Germany's Federal Office for the Protection of the Constitution (BfV) were both carried out through individual national procurement processes. This demonstrates that even within familiar contract and procurement procedures, requiring a vendor's ownership structure and network configuration as conditions can produce substantive isolation. Before the law could catch up, individual nations changed the architecture itself, and the next challenge for the European Union was to translate these individual cases into common procurement standards.

The European Commission is seeking to codify this principle of isolation into procurement regulations rather than leaving it to the choice of individual companies. The proposed Cloud and AI Development Act unveiled by the Commission in June 2026 is still a draft bill subject to deliberation by the European Parliament and the Council, not an enacted law. Nevertheless, the proposal sets a direction that requires isolation to be proven through the design of the system itself rather than contractual promises, establishing a tier system that evaluates a vendor's ownership structure, the nationality of its board members, and whether external entities have access to its source code.

At the highest tier, proposals are being discussed that would require a level of isolation allowing zero foreign capital interference throughout the entire process of system

design and source code maintenance.

For such an evaluation system to be meaningful, the verification process itself cannot rely merely on vendor self-reporting. France's existing proprietary certification standard, SecNumCloud, employs a method where government-designated auditing bodies regularly audit software design blueprints and source code. Affixing a label like "air gap" or "sovereign cloud" does not mean isolation is complete. Only when external auditors can directly inspect network diagrams, equity ownership registries, and source code repositories does that label take on real substance.

The proposed Cloud and AI Development Act also includes a measure requiring top-tier qualification under the certification framework operated by the European Union Agency for Cybersecurity (ENISA), designing a dual structure where national-level certification and Union-level certification jointly verify isolation.

Contracts and architecture do not substitute for one another; they must work together. Contracts remain necessary today as documents specifying procurement prices, service quality, and liability. However, in domains such as national security where even the possibility of foreign government intervention must be blocked, if physical system configurations and ownership structures fail to back up the protections promised by a contract, those promises will not hold in a moment of crisis.

Contractual provisions function only when the counterparty is willing to keep its promises. America's CLOUD Act and Section 702 of the Foreign Intelligence Surveillance Act demonstrate that the U.S. government already holds the authority to revoke that willingness over American corporations, and the Fable 5 access block incident proved that this authority can actually be exercised against allies. European intelligence agencies and administrative departments turned to air gaps and ownership-structure isolation because they experienced firsthand the gap between the protections promised on paper and those actually produced by network design.

Bridging that gap does not end with a single legal clause; it is completed only when three conditions come together: years of migration, in-house maintenance, and independent auditing.

Sources and References

1. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, June 17, 2026, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

2. Todd Spangler, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, July 22, 2025, https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-

authorities/

3. Author unknown, 'Confirmed and Summarized the Trend of Europe's Departure from Palantir Down to Primary Sources' (Yureobui Palrantieo ital heureumeul won soseukkaji hwaginhae jeongrihaetsseumnida), 2026.

4. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, June 16, 2026.

5. Loïc Duval, 'La DGSI remplace Palantir par ChapsVision', InformatiqueNews, June 18, 2026.

6. Author unknown, 'La DGSI prépare la sortie progressive de Palantir au profit de ChapsVision', Solutions Numériques, June 17, 2026.

7. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

8. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), July 7, 2026.

9. No source (supplementing general knowledge). (→ Supplements the conceptual difference between data localization and technical isolation, and the general technical principle that air-gapped systems are disconnected from real-time updates and economies of scale of external clouds, bearing their own maintenance burden.)

3.1 The Difference Between the Domestic Intelligence Sphere and the Military Alliance Sphere

On June 16, 2026, French Prime Minister Sébastien Lecornu announced that France's General Directorate for Internal Security (DGSI) would migrate from the software provided by the American company Palantir to ArgonOS, developed by the French firm ChapsVision. On the same day, Le Monde reported that Palantir claimed its contract with the government remained valid. The announcement, the contract termination, and the actual system replacement are separate procedures occurring at different times. The news on June 16 was a declaration of initiating the transition, not confirmation that the migration to ArgonOS had been completed.

Germany's Federal Office for the Protection of the Constitution (BfV) followed a similar path. In May 2026, multiple German media outlets reported that the BfV decided to adopt ChapsVision's ArgonOS to replace American surveillance software. The Netherlands Ministry of Defence unveiled a plan in June 2026 to completely remove Palantir software within the next two years. Swiss federal agencies reportedly rejected intelligence bids submitted by Palantir at least nine times between 2018 and 2025. These rejections in Switzerland were not hasty decisions made by a single government, but procurement judgments repeated over several years.

A similar trend emerged in Spain. Interior Minister Fernando Grande-Marlaska halted a data analytics project jointly pursued by Spain's Civil Guard (Guardia Civil) and Palantir. A 16.5 million euro contract signed by Spain's Military Intelligence Center in 2023 was not renewed after it expired. Although top military leaders requested to maintain the contract, their request was denied. Instead, the Spanish government decided to spend 720 million euros through its domestic Technology Transformation Corporation to build an independent artificial intelligence data center. The Belgian government announced that it would invest 1 billion euros by 2029 to construct its own military data storage facility.

In the United Kingdom, the conflict surfaced more prominently. The UK House of Commons Science, Innovation and Technology Committee released a report pointing out that handing over public data analytics networks to a private American company was a security vulnerability. Regarding a 330 million pound contract signed between the UK's National Health Service (NHS) and Palantir, members of Parliament demanded that the agreement be terminated. They highlighted the issue that despite paying such a substantial sum, the government had not received the ontology authority to design the

data architecture. This means that even after the contract ends, no technological assets remain in the hands of the UK government.

The House of Commons advised the government to cut ties with Palantir based on a sovereignty-based termination clause that takes effect in February 2027. In Denmark's Parliament, opposition parties also introduced a motion in May 2025 calling to end reliance on American software.

All these decisions were made within individual countries. Domestic intelligence agencies and defense ministries hold the authority to manage their own police records and intelligence data. Terminating contracts and migrating to products from another company can also proceed relatively quickly under that authority. There is a legal reason for this. The CLOUD Act, enacted by the U.S. Congress in March 2018, stipulates that if a service is operationally controlled by a U.S. corporate entity, data must be surrendered upon a formal request from U.S. investigative authorities, regardless of which country the server storing the data is located in.

Whether this provision was actually applied to specific cases and whether each request was lawfully processed are issues that must be evaluated on a case-by-case basis. However, the mere existence of this law led European intelligence agencies to view keeping their domestic investigative data within the server architecture of American companies as a burden.

During the same period, decisions within the multilateral military alliance moved in the opposite direction. In 2025, the NATO Communications and Information Agency (NCIA) signed a contract to deploy Palantir's Maven Smart System at Allied Command Operations. This contract took approximately six months from defining requirements to signing. More than a year later, in June 2026, the NATO Security Accreditation Board confirmed the system's full technical operational capability. The point at which the procurement contract was signed and the point at which full operational capability was certified were not the same event, and there was a long period of validation and testing between them.

This difference arises because the structural nature of the work handled by the two spheres is fundamentally distinct. A system used by a single domestic intelligence agency is accessed only within that nation's borders by agents bound by that nation's laws. Case records created by an investigator at France's General Directorate for Internal Security (DGSI) are stored in French within ArgonOS and leave the system only through the procedures of French prosecutors and courts. By contrast, the Maven Smart System was designed from the beginning so that military personnel from more than thirty countries look at the same screen and share the same target list.

Colonel Arnel David of the U.S. Army stated that more than 50 tactical applications had been developed within this system, and these programs were built to comply with STANAG 4774 and 4778, the communication standards of NATO Allied forces. Complying with these standards means that coordinates entered by a Polish soldier can be read immediately by a Norwegian soldier, allowing a U.S. pilot to navigate using those exact coordinates. Domestic investigative records are secure only when they do not cross borders, whereas target information for allied operations is useful only when it does cross borders. The security criteria for these two functions point in opposite directions.

Top NATO officials explain this difference not as a political choice, but as a military necessity. Admiral Pierre Vandier of the French Navy, NATO's Supreme Allied Commander Transformation, acknowledged that European militaries do not yet possess their own software suitable for automatically analyzing satellite imagery and coordinating ammunition supply. He stated that the alliance's operational capabilities cannot be compromised before alternative technology matures. Other commanders, including General Kai Rohrschneider, warned that if member states use different systems, connectivity between encrypted communication networks could be severed.

Their logic is that if a single nation weakens the communication system of the entire alliance in trying to protect its own digital sovereignty, the resulting damage will be far greater.

Rebuttals to this logic naturally follow. The reason member states excluded Palantir from their domestic security spheres is that U.S. domestic law grants U.S. investigative authorities access to the servers of American companies. If this concern is taken seriously within domestic intelligence networks but ignored within the NATO command structure, the criteria are divided not by the nature of the data, but by whether the contracting party is a domestic agency or a multinational alliance.

This contradiction is also evident in the movement of capital. According to a report by the German online media outlet netzpolitik.org, banks and asset management firms across several European countries actually increased their purchases of Palantir stock even while their own governments were distancing themselves from the company. In its Q2 2026 earnings report, Palantir stated that its revenue had grown by 93 percent compared to a year earlier. The public sector walked away from Palantir, while private capital drew closer to it during the exact same period.

Prior to this, on February 16, 2023, Germany's Federal Constitutional Court ruled unconstitutional HessenDATA, an automated data analysis system built by the Hessen State Police based on Palantir's Gotham engine. The court ruled that this system, which automatically combined personal data to identify dangerous individuals, lacked a

sufficient legal basis. Issued even before the European Union Artificial Intelligence Act was established, this ruling demonstrated early on that a domestic constitutional order can regulate artificial intelligence systems for domestic policing, separate from national security exceptions.

The constitutional court of a single country holds the power to put the brakes on its own police system. However, in an allied command system shared by thirty-two countries, there is no single institution equipped with such a braking mechanism. The divergence between the departure from the domestic intelligence domain and the expansion of the military alliance domain stems from the difference between a domain with a controlling authority and one without.

Sources and References

1. French Senate Commission of Inquiry, 'Analysis Report on Major EU Countries' Move Away from Palantir and Digital Sovereignization' (Yuropeonyeonhap(EU) Juyogugui Tal-Palrantieo Haengbowa Dijiteol Jugwonhwae Gwanhan Bunseok Bogoseo), French Government Official Portal, 2026.

2. John Henry, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, June 16, 2026.

3. Unknown Reporter, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, June 17, 2026.

4. Unknown Author, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, May 26, 2026.

5. IT-Daily Editorial Department, 'Palantir: Bundesamt für Verfassungsschutz wählt ChapsVision', IT-Daily, May 2026.

6. Colin Barker, 'Defensie wil binnen twee jaar af van Palantir-software', ICTMagazine, June 3, 2026.

7. Eglė Krištopaitytė, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, July 2, 2026.

8. Le Soir Editorial Department, 'Palantir s'implante en Belgique: 28 questions à (se) poser', Le Soir, March 19, 2026.

9. Novara Media Editorial Department, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026.

10. UK House of Commons Science and Technology Committee, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', UK Parliament, 2026.

11. Jan Eberle, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026.

12. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, 2026.

13. Federal Constitutional Court of Germany, 'Decisions search - Judgment of 16 February 2023', Federal Constitutional Court of Germany, February 16, 2023.

14. Unknown Author, 'Data Compiled by Verifying Europe's Departure Trend from Palantir Back to Original Sources' (Yuropeui Palrantieo Ital Heureumeul Won Soseukkaji Hwaginhae Jeongrihan Jaryo), 2026. (Based on Switzerland's nine bidding rejections and Danish opposition proposal)

15. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE Official Press Release, June 30, 2026.

16. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.

17. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018.

3.2 NATO's Acquisition of Full Operational Capability for the 'Maven Smart System (MSS)' and the Interoperability Trap

In 2017, the U.S. Department of Defense launched Project Maven to locate military targets by analyzing drone and satellite imagery using artificial intelligence. Palantir built a commercial version using this initiative as a stepping stone, and this commercial version forms the foundation of the Maven Smart System adopted by NATO.

In 2025, the NATO Communications and Information Agency (NCIA) signed a contract with Palantir to use this system at Allied Command Operations. The period from defining procurement requirements to signing the contract took about six months. What NATO secured at this point was the right to use the system and a contract, not certification allowing its unrestricted use across all military activities.

Full technical operational capability, or Full Operational Capability (FOC) certification, came more than a year later. On June 22, 2026, the NATO Security Accreditation Board confirmed that the Maven Smart System reached the operational level required for classified networks. Bart van Miert, acting Chief Operating Officer of the NCIA, reported these certification results to allied headquarters on June 26. Supreme Headquarters Allied Powers Europe (SHAPE) officially announced on June 30 that the system could be used without restriction across all military domains, including exercises and real-world operations.

General Manager Dylan Browne of the NCIA stated that he was proud of the collaboration that delivered this capability to allied warfighters.

Between the signing of the contract in 2025 and the certification of full operations in 2026, there was a period of verification. The system underwent real-world operational scenarios during the multinational exercise Steadfast Deterrence, which concluded in Norway on May 13, 2026. Major General Ruprecht von Butler of the German Bundeswehr stated that during this exercise, he confirmed the artificial intelligence's performance in automatically generating behavioral scenarios for simulated enemy forces.

The Maven Smart System collects and analyzes data sent by military satellites, drones, and radars in real time. Viewing this display, military personnel can significantly reduce the time needed to select strike targets. Colonel Arnel David of the U.S. military

stated that more than 50 tactical applications have been developed within this system, and these programs were built to comply with STANAG 4774 and 4778, the allied communication standards. Complying with these standards means that member state militaries can securely exchange target information with armed forces of other nations.

Palantir took a clear position on the issue of data ownership. Fiona Bradley, seconded from Palantir, stated that ownership of all software and data within the Maven Smart System belongs to the NATO alliance, adding that her company does not arbitrarily process and resell customer data. While this explanation answers the question of who owns the data, it fails to answer a different question: who designs the architecture of the programs that handle that data.

The authority to modify the system's core code and data classification schema, namely its ontology, remains with Palantir's civilian engineers. Target coordinates entered by soldiers of NATO member nations are contractually the alliance's asset, yet the method of organizing and classifying those coordinates operates strictly within the framework set by Palantir. To use a library analogy, it resembles a structure where the library owns the books, but a Palantir employee still occupies the librarian's chair, determining the order in which the books are categorized and shelved. Data ownership and system design authority are not the same kind of sovereignty; NATO secured the former, while the latter remains inside Palantir.

The performance of this system was put to the test in actual operations. In February 2026, the U.S. military prepared airstrikes targeting Iran-linked armed groups. During the first 24 hours after launching the strikes, the military ran the Maven Smart System to identify more than 1,000 potential strike locations. Observing these results, allied commanders expressed confidence in the processing speed of the American software.

During the same period, France, Germany, and the Netherlands were making the exact opposite decisions in their domestic spheres. France declared on June 16 that it would migrate the software of France's General Directorate for Internal Security (DGSI) to ArgonOS, and Germany's Federal Office for the Protection of the Constitution (BfV) made the same decision in May. In April, Vice Admiral Thomas Daum of the German Bundeswehr excluded Palantir from the final procurement specifications of the defense cloud project. While upper NATO leadership moved deeper into Palantir's system, domestic intelligence and defense procurement networks in those very same countries were stepping further away from the company.

These movements in two opposing directions generated friction within NATO. General Vandier acknowledged that European militaries do not yet possess proprietary software capable of matching Palantir in analyzing satellite imagery or coordinating

ammunition supplies. He stated that the alliance's operational capabilities cannot be compromised before alternative technologies mature. Lieutenant General Kai Rohrschneider of Germany warned that if member nations use independently developed domestic systems, there is a risk of breaking connections between encrypted communication networks.

In response, France began experimenting with its own alternatives. In June 2026, the French Ministry of Defense tested the Arcadia platform during a procurement exercise held in Poland. Arcadia is battlefield awareness software jointly developed by French defense firms Thales and Safran, alongside Mistral AI. General Patrick Justel, Deputy Chief of Staff of the French Army, noted that NATO's practice of accepting foreign systems without significant scrutiny threatens national information security. The leaders of France and Germany signed a joint declaration on July 17, 2026, to establish Europe's own sovereign digital backbone.

It will take time for Arcadia to establish itself enough to replace the Maven Smart System. In the meantime, interoperability requirements within the NATO command structure will continue to pressure member states to share target intelligence and align communication standards, pulling procurement toward Palantir's system, which is already battle-tested and compliant with standards. Domestic intelligence agencies can make decisions and conclude contracts within their borders, but a command structure shared by 32 nations cannot be altered at will by a single country. This difference is why interoperability within NATO continues to override national control.

Sources and References

1. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.

2. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE official press release, June 30, 2026.

3. Tamara Rozouvan, 'Maven Smart System achieves full operating capability with NATO', Janes, July 1, 2026.

4. Nuray Taylor, 'NATO's 'Digital Lethality Branch' Breaks Records in Drive for Alliance-Wide Interoperability', AFCEA International, July 31, 2026.

5. Fernando Castro de Beiro, 'Foreign software, Europe's War: How Maven and Palantir are already making decisions for Europe', DigitalShield, July 15, 2026.

6. Wikipedia, 'Palantir', last revised August 9, 2026.

7. Unknown reporter, 'Spain blacklists Palantir over domestic security concerns', The Cradle, August 3, 2026.

8. Eglė Krištopaitytė, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, July 2, 2026.

9. T.Wiegold, 'Cyber-Kommandeur der Bundeswehr lehnt Software von Palantir ab', Augen geradeaus!, April 28, 2026.

10. Cybernews Editorial Board, 'France and Germany to build an alternative to Palantir', Cybernews, July 20, 2026.

11. John Henry, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, June 16, 2026.

12. Unknown author, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, May 26, 2026.

3.3 Security Exemption Clauses and Control Blind Spots in the European Union Artificial Intelligence Act (AI Act)

The AI Act varies regulatory stringency based on the level of risk an artificial intelligence system poses to humans. Higher-risk systems face heavier obligations for transparency, risk assessment, and human oversight. Article 2 of the regulation specifies that the law does not apply to AI systems placed on the market or used exclusively for military, defense, or national security purposes. This exemption applies regardless of whether the entity developing or operating the system is a government agency or a private enterprise. Recital 24 outlines the rationale.

National security is the sole responsibility of individual member states under the European Union treaty framework, while military and defense activities are governed separately under the EU's Common Foreign and Security Policy by their nature.

This exemption clause was not an accidental loophole left behind during negotiations, but the result of active demands from member states. According to a Spring 2026 report by the Centre for Future Generations, France, alongside Italy and Sweden, led lobbying efforts to expand the scope of exemptions on national security grounds. These governments wanted law enforcement authorities to use facial recognition cameras or biometric surveillance tools in public spaces without undergoing risk assessment procedures in Brussels. As a result, domestic law enforcement intelligence networks and military alliance target identification systems both fell outside the scope of the AI Act.

Prime examples of systems operating within this blind spot include Gotham-series programs used for domestic law enforcement and NATO's Maven Smart System. Requirements mandated by the AI Act for other high-risk systems (such as documentation obligations, procedures to track malfunctions and bias, and human review of final decisions) are not legally binding for these two systems. When the NATO Security Accreditation Board granted full operational certification to the Maven Smart System in June 2026, the procedure did not undergo review under this law.

However, this exemption is not the same as deregulation. The Article 2 exemption applies only when a system is used strictly for military, defense, or national security purposes. Even if the same software from the same company is deployed for non-military purposes, such as public administration or civilian policing, it falls under the

AI Act. The exemption is not a label attached to a specific company or customer, but a condition tied to the actual intended use of the AI.

The absence of the AI Act does not mean there are no other legal mechanisms in place. On February 16, 2023, before the AI Act was even enacted, Germany's Federal Constitutional Court ruled that Hessendata, the automated data analysis system used by the Hesse State Police, was unconstitutional. The ruling established the principle that even AI systems justified by national security or law enforcement must have a distinct legal basis within each country's constitutional order. The national security exemption in the AI Act simply means this specific regulation does not apply; it does not eliminate member states' constitutions, data protection laws, or parliamentary oversight powers.

The situation at the NATO level is not a complete legal vacuum either. The fact that the Maven Smart System required approval from the NATO Security Accreditation Board shows that NATO's own certification procedure fills the space left by the AI Act. However, this certification process evaluates whether the system operates safely under military criteria; it is not designed around standards like bias checks or transparency obligations to citizens required by the AI Act. The oversight entity and standards have shifted, but oversight itself has not disappeared.

However, because this oversight falls under military secrecy, public access to scrutinize the results is far more restricted than in domestic intelligence.

In January 2026, the European Parliament voted to pass a technological sovereignty resolution aimed at reducing dependence on a small group of American tech companies. Lawmakers cited the risk that an overconcentration of data in US companies like Microsoft and Amazon could allow a single US government decision to halt European services. The US administration pushed back against these European regulatory moves, hinting at potential trade retaliation.

On July 17, 2026, the leaders of France and Germany signed a joint declaration to build Europe's own sovereign digital backbone. The declaration points toward completing indigenous software projects such as Arcadia. The national security exemption in the AI Act acknowledges that regulation alone cannot halt Europe's reliance on American technology; it does not resolve that reliance. Filling the space beyond the reach of regulation remains the responsibility of alternative technologies built by Europe itself.

Sources and References

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, Article 2 and Recital 24, December 13, 2024.

2. Centre for Future Generations, 「Enforcement spotlight - Spring 2026」, Centre for Future Generations, Spring 2026 issue, pp. 2-3.

3. Federal Constitutional Court of Germany, 'Decisions search - Judgment of 16 February 2023', Federal Constitutional Court of Germany, February 16, 2023.

4. French Senate Inquiry Commission, 'Analysis Report on the Move Away from Palantir by Major European Union (EU) Countries and Digital Sovereignty (Yureobyeonhap(EU) Juyogugui Tal-Palantir Haengbowa Dijiteol Jugwonhwa-e Gwanhan Anseok Bogoseo)', French Government Official Portal, 2026.

5. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE Official Press Release, June 30, 2026.

6. Netherlands Ministry of Defence and European Technology Council, 'Material compiling and verifying the flow of Europe's Palantir departure down to original sources', 2026.

4.1 The Cloud and AI Development Act (CADA) and Regulatory Innovation in Data Center Acceleration Zones

On June 3, 2026, the European Commission formally presented the Cloud and AI Development Act proposal, abbreviated as CADA. Its document number is COM(2026) 502. One thing must be made clear from the start: CADA is not yet law. It is a proposed regulation submitted by the European Commission to the European Parliament and the Council of the European Union for deliberation, and as of August 11, 2026, when this book is being written, it has not been formally adopted.

In the European Union, a regulation, unlike a directive, is a powerful legal instrument that takes effect directly without requiring separate legislation by member state parliaments. The deliberation process to finalize a regulation is therefore rigorous. Under the ordinary legislative procedure, provisions are finalized only after the European Parliament and the Council submit their respective amendments and vote on them. In that process, the provisions and figures in the current proposal may change. The four sovereignty assurance levels, acceleration zones, and termination rights discussed in this chapter are all blueprints at the proposal stage, not norms that currently bind member state governments and businesses.

This distinction is also necessary to avoid confusing CADA with the European Union Artificial Intelligence Act (AI Act, Regulation (EU) 2024/1689). The AI Act is a regulation enacted in 2024 that is already in force, classifying artificial intelligence systems by risk level and imposing corresponding obligations. CADA, by contrast, is a separate proposal addressing the infrastructure and procurement procedures where that artificial intelligence will run, and as of August 2026, it has not been enacted. One should not treat the legal status of both laws as identical simply because the words artificial intelligence appear in both their titles.

One is a norm already in effect, while the other is a proposal still awaiting deliberation.

CADA emerged as part of the AI Continent Action Plan pursued by the Commission. The goals of the plan come down to two things: increasing computing power in data centers within Europe and protecting that computing capacity from foreign jurisdictions outside Europe. The structure of the European cloud market explains why these two goals were bundled into a single bill. Industry reports indicate that Amazon, Microsoft, and Google account for an overwhelming share of the European cloud infrastructure services market, while companies headquartered in Europe hold a far smaller portion.

On June 15, 2026, tech policy outlet Tech Policy Press noted in an article that this concentration creates a security vulnerability by placing the fate of public systems under foreign judicial jurisdiction.

Europe tried similar approaches before CADA. Launched in 2019 under the leadership of France and Germany, Gaia-X was a private sector-led project aimed at creating a data infrastructure standard that European companies could share. But Gaia-X was a voluntary initiative without legal force, and conflicting interests among participating companies prevented it from delivering its intended results. What sets CADA apart from Gaia-X is that it seeks to move the procurement market itself through a legally binding regulation rather than a voluntary standard.

Yet because that regulation must pass deliberation by the European Parliament and the Council to gain real force, CADA also remains at the stage of a declaration of intent for now.

This concept may be unfamiliar to general readers. Computer systems used by governments, hospitals, or police departments do not necessarily run in buildings located within that country's borders. When using cloud services rented from companies like Amazon, Microsoft, or Google, actual computing takes place in massive server facilities built across the globe. In the industry, these ultra-large server facilities are called hyperscalers. Even if a server building physically stands on European soil, if the company that owns and operates it is a US entity, legal demands from the US government can reach the data hosted on it.

This gap between physical location and legal control is the central issue threading through this entire chapter.

In addition, the cloud industry experiences a phenomenon known as data gravity. Once large amounts of data move to a specific company's cloud, keeping other programs and services that process that data within the same cloud becomes faster and cheaper. Over time, data and applications managing it become increasingly intertwined inside a single company's ecosystem. Public institutions often start by renting basic storage space, only to find a few years later that their administrative operations cannot function without that company's cloud.

This is why European policymakers worry more about the depth of this entanglement than about market share statistics.

The competitiveness report submitted to the European Union in September 2024 by former European Central Bank President Mario Draghi is frequently cited as a document warning of this issue in advance. The Draghi Report recommended that

Europe secure computing capacity with guaranteed sovereignty if it is to independently develop artificial intelligence and operate services. This recommendation reappears repeatedly across European Commission policy documents. The starting point of the CADA proposal is the recognition that having servers inside Europe is not enough, and that one must also scrutinize the nationality and governance structure of the company controlling those servers.

The Commission is pursuing this data center expansion target alongside a separate project called AI Gigafactories. AI Gigafactories refer to ultra-large computing facilities equipped with massive graphics processing unit clusters, a concept introduced in the AI Continent Action Plan. Behind this initiative is the goal of securing computing power capable of training large artificial intelligence models from start to finish within Europe, rather than merely increasing the number of servers. Until now, European researchers and companies had to rent computing resources provided by US cloud providers to train large models.

CADA and the AI Gigafactories initiative represent an attempt to alter this rental structure itself.

It is also worth noting that some of the infrastructure supporting this goal is already operational. The European Union has operated supercomputers jointly with member states through the EuroHPC Joint Undertaking since 2018. Projects to convert existing supercomputers, such as LUMI in Finland or MareNostrum in Spain, into computing resources for AI training began even before CADA was introduced.

The CADA and AI Gigafactories design does not completely replace these existing assets, but rather expands their scale by bringing in additional private capital and member state budgets.

The numerical target for CADA set by the European Commission is clear: to more than triple the European Union's data center capacity over the next five to seven years. With this expanded capacity, the goal is to meet the demands of businesses and public administration by 2035. This objective is included in the Commission's proposal document itself. The reason for setting such an ambitious target is that the gap between supply and demand is already widening.

The "European Technological Sovereignty and Digital Infrastructure" document adopted by the European Parliament on January 22, 2026, projected that a significant portion of global electricity consumption comes from data centers and telecommunications facilities, and that the share of electricity consumed by European data centers will increase noticeably over the next few years. As artificial intelligence

computing grows in earnest, this share will rise even more steeply. If the pace of building data centers fails to keep up with demand, Europe will find it difficult to break free from relying on American or Chinese clouds for AI development.

The problem is that building data centers is inherently slow. Repeated reports have highlighted instances where complex permitting procedures, land regulations, and environmental impact assessments held back projects whenever member states attempted to build new data storage facilities for public administration. A joint report published on April 27, 2026, by Germany's Federal Office for Information Security (BSI) and international law firm Bird & Bird noted that discrepancies in administrative procedures between the German federal government and state governments cause delays starting right at the procurement specifications stage. Such delays are not unique to Germany.

Plans to construct large-scale cloud servers have been repeatedly scaled down or scrapped across several European countries due to local opposition or delayed environmental reviews. While it takes years in a single region just to select a data center site, secure power supply, and obtain permits, computing demand grows at a far faster pace.

The CADA proposal places procedural innovation at its core to cut these delays. In a report on June 4, 2026, political news outlet Politico Europe stated that CADA recommends member state governments designate sites with favorable geography and power grid conditions as Data Center Acceleration Zones. An overview report on the technological sovereignty package compiled by law firm Bird & Bird also confirmed the proposal's intent: within these acceleration zones, permitting procedures will be consolidated into a single window, and maximum deadlines will be set for processing. Rather than visiting multiple authorities separately, operators can have their project's entire lifecycle coordinated through a single point. The procedures this single window aims to integrate are diverse.

The plan aims to coordinate procedures previously handled separately by different agencies—such as power grid connection approvals, water and cooling water supply permits, building safety reviews, and telecommunications line entry permits—through a single window. Until now, operators had to go through these procedures step by step in sequence, meaning a delay at one stage pushed back all subsequent steps. According to reports, the deadline for processing permits for facilities handling confidential data within these acceleration zones will be capped at a maximum of 18 months.

Considering that permitting procedures for constructing a single large facility frequently took several years, this cap signals a fundamental restructuring of the

process itself.

The same report notes that environmental impact assessment procedures were also designed to be simplified for projects within acceleration zones. Whether this simplification amounts to an actual exemption from environmental review or merely reduces the review period will be clarified as the proposal undergoes deliberation by the European Parliament and the Council. It is premature at this stage to draw conclusions based on finalized statutory language. However, the direction is clear: infrastructure projects directly tied to national security will take precedence over routine local government permitting procedures.

Authority to designate sites as acceleration zones primarily rests with member state governments. Under this system, local or central governments select sites with available grid capacity, telecom line accessibility, and physical security, and propose them to the European Commission, which reviews and incorporates them into a final list. This procedure is viewed as borrowing a framework similar to the foundry site designation method already used under the Chips Act.

This expansion goal ties directly into the European Union's climate targets. The EU set a binding target to achieve carbon neutrality by 2050 through the European Green Deal. To maintain this goal as data center power consumption grows, pressure follows to power a significant portion of newly built facilities with renewable energy. That CADA links the privileges of acceleration zones to sustainability standards can be read as a signal that climate goals will not be sacrificed for speed.

Risks also accompany the acceleration zone concept. Privileges that fast-track procedures can lead to a waste of tax dollars if mechanisms are lacking to verify whether receiving projects truly serve the public interest. In Sweden, after the government granted tax incentives to data center companies in 2022 to expand national tech infrastructure, criticism followed that procedures to verify whether those companies actually adhered to renewable energy usage plans were inadequate. Swedish media outlet SecurityUser.com revisited this issue in March 2026, reporting that Nordic countries are redesigning their digital sovereignty infrastructure policies.

To avoid repeating such failures, the CADA proposal includes safeguards requiring operators receiving acceleration benefits to prove compliance with sustainability standards, according to the Bird & Bird report. In exchange for cutting procedural steps to gain speed, it imposes a new obligation to verify outcomes.

The financial scale reveals that CADA does not operate in isolation. An accompanying document (COM(2026) 555 final/2) released alongside by the Commission on June 3,

2026, estimated that fully implementing the Cloud and AI Development Act and the Next-Generation Security Package will require investments totaling 300 billion euros by 2036. Of this amount, 200 billion euros will be allocated to data center infrastructure expansion. The document projected that an additional 100 billion euros will be set aside for semiconductor foundries and AI gigafactories.

This investment plan is not intended for the Cloud and AI Development Act alone. While the European Chips Act, which took effect in 2023, addressed expanding semiconductor manufacturing capacity, CADA's financial plan functions more like a follow-up effort addressing the data centers and artificial intelligence infrastructure that will run on those chips. Industry analysis report innobu explained that these two laws bind together to form Europe's technological sovereignty package. These figures remain estimates by the Commission, and the actual budget will be finalized after budget negotiations between member states and the European Parliament.

The gathering of European Union leaders in Berlin on November 18, 2025, to issue a joint declaration at a security summit is cited as the political background for this financial plan.

The nature of the threat addressed by this infrastructure expansion differs from the blockage of model access examined in Chapter 2. The incident in which Anthropic temporarily suspended foreign access to Fable 5 was something that occurred at the software layer. A single export control directive from the US government blocked access permissions to a specific model altogether. By contrast, the threat arising from not owning data centers is more fundamental. If a country is in the position of borrowing computing power itself from foreign companies, access to the hardware running the model—rather than just the model itself—can be cut off. What CADA targets is this vulnerability at the hardware layer.

Synthesizing reporting from Bird & Bird and the IT media outlet ITWelt, the CADA proposal reportedly set a target encouraging a significant portion of private companies within Europe to migrate to sovereign cloud services by 2030. The initiative also discusses plans to densely deploy low-latency edge computing hubs across the continent to reduce reliance on major US platforms in the consumer service domain as well. Whether these targets will remain binding obligations in the final regulation or be softened to recommendations remains to be seen during the review process.

This prioritization comes at the cost of diminishing the voice of local communities. If a data center is designated as a strategic project of national importance, the scope for residents near the site to file objections or participate in public hearings—rights they could normally exercise during standard urban planning procedures—may be

narrowed. Shortening procedures for the sake of speed also means reducing the voices of local residents within those procedures. How CADA will ultimately strike this balance has not yet been settled.

Member states also differ in their approaches to securing power. France, which has a high share of nuclear power generation, is pushing a policy to construct data centers near nuclear power plants. Providing stable, low-carbon electricity directly to data centers is cited as the key advantage of this approach. By contrast, countries that have restructured their power grids around renewable energy must figure out separately how to align the intermittency of solar and wind energy with the 24-hour operational demands of data centers. The inclusion of power grid conditions in CADA's criteria for designating acceleration zones appears to be designed with these differing national circumstances in mind.

The possibility that acceleration zone designations could concentrate in specific member states is also being discussed. Parts of Western and Northern Europe, where power grids and telecommunications infrastructure are already well established, are likely to meet the designation criteria first, while parts of Eastern and Southern Europe, where infrastructure investment is relatively slow, risk falling behind. How to harmonize the European Union's principle of balanced regional development with the logic of speed in data center acceleration remains a challenge that CADA must address as it refines its final text.

The picture painted by CADA ultimately narrows down to a single question. If Europe cannot build the physical spaces to store its own data, discussing sovereignty over the software running on top of it becomes empty. On top of the foundation of physical data centers lies yet another layer. It is the criterion that determines who controls those data centers.

Sources and References

1. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

2. European Commission, 'Cloud computing', 2026, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

3. Cecilia Rikap, 'Does Europe Really Have a Plan for Tech Sovereignty?', TechPolicy.Press, June 15, 2026, https://www.techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty-cada/

4. Mario Draghi, 「The Future of European Competitiveness」, European Commission, September 2024.

5. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', Official Journal of the European Parliament, January 22, 2026.

6. German Federal Office for Information Security, 「Digitale Souveränität bei IT-Vergaben: Zwischen politischem Anspruch und vergaberechtlicher Wirklichkeit」, Bird & Bird Insights, April 27, 2026.

7. Tyler Weygold, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, June 4, 2026, https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/

8. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, June 23, 2026.

9. SecurityUser.com, 'Ny molnpolicy ska ge ökad digital suveränitet i offentlig förvaltning', SecurityUser.com, March 2026.

10. European Commission, COM(2026) 555 final/2, Official Journal of the European Union, June 3, 2026.

11. innobu, 'EU Tech Sovereignty 2026: Chips Act 2.0 and CAIDA', innobu Insights, June 2026.

12. Itwelt Editorial Department, 'Best European cloud alternatives: Top 10 of 2026', Itwelt, February 2026.

4.2 Design of CADA's Four-Tier Sovereignty Assurance Levels

The second pillar established by the CADA proposal is not the physical shell of the data center, but the criteria for determining the software running inside it and the nationality of the company operating it. The European Commission presented these criteria divided into four tiers. In English, they are called Sovereignty Assurance Levels, abbreviated as SEAL. A report published on July 7, 2026, by the Bloomsbury Institute for Security and Intelligence (BISI), a security policy research institute in London, defined this four-tier structure as one of CADA's three pillars, explaining that its design purpose is to block the influence of the U.S. CLOUD Act and Section 702 of the Foreign Intelligence Surveillance Act on European public data.

The CLOUD Act, passed by the U.S. Congress in 2018, obligates information and communications service providers controlled by U.S. corporations to preserve and disclose records to law enforcement agencies regardless of which country the data is stored in. This provision, verified in the text of the legislation and congressional summaries, can also apply to subsidiaries of U.S. companies established within Europe. Even if a provider enters into a contract with a European entity, keeps servers on European territory, and complies with European data protection laws, if the parent company of the corporation operating those servers is a U.S. corporate entity, U.S. law enforcement requests can take precedence over contractual terms.

The staff working document (SWD(2026) 502 final) issued by the European Commission alongside the CADA proposal reportedly analyzed this issue of extraterritorial jurisdiction in detail.

The SEAL framework must not be confused with data protection law. The European Union's General Data Protection Regulation (GDPR) is a law governing how personal data should be collected and processed, and it has already been in force since 2018. Complying with GDPR does not resolve the issue of the nationality of the company handling that data. No matter how securely data is encrypted and collected only to the extent necessary, if the company storing that data is a U.S. corporation, GDPR's protections reveal their limits when faced with legal demands from the U.S. government. What GDPR regulates is the manner of handling data, whereas what SEAL seeks to regulate is the nationality and ownership structure of the company handling that data.

The two laws look at the same data from different dimensions.

European courts have already confronted this issue head-on once before. In July 2020, in the so-called Schrems II ruling, the Court of Justice of the European Union invalidated Privacy Shield—the personal data transfer agreement between the European Union and the United States—citing U.S. surveillance laws that allow American intelligence agencies access to communications data. The core of this ruling was that no matter how meticulously data protection clauses are written into a contract, as long as the counterparty to that contract is subject to U.S. law, access by American intelligence agencies cannot be blocked by contract alone.

This accumulated judicial experience forms the backdrop for CADA's decision to classify sovereignty tiers based on criteria far more fundamental than contractual provisions: nationality and ownership structure. The security lesson Europe learned was that ultimately, a company's ownership structure and nationality, rather than contractual phrasing, serve as the effective shield.

This lesson also influenced market responses. In recent years, Amazon, Microsoft, and Google have each launched sovereign cloud products under their own branding, targeted at European customers. Promises to store and process data strictly within Europe and to restrict access by non-European employees are common advertising points for these offerings. However, it is rare for such products to transfer controlling shares and board voting rights to Europe as required by SEAL's higher tiers, Level 3 and Level 4. Europeanizing server locations and operating regulations is a commitment of an entirely different order from Europeanizing company ownership itself.

What the SEAL framework aims to do is precisely to distinguish between these two dimensions and specify them in procurement standards.

As a specific example, Amazon Web Services announced the European Sovereign Cloud in 2023, establishing a separate European entity with a board of directors and management team composed of European citizens. It was a commitment to keep data storage and operational staff within Europe. However, ultimate ownership of this European entity remains in the hands of its parent company, Amazon.com, in the United States. Because Level 3 and Level 4 of SEAL require even this ultimate ownership structure to transition to European ownership, this form of sovereign cloud product may qualify for lower tiers but will struggle to cross the threshold of the higher tiers.

Level 1 of SEAL requires the most basic conditions: that data storage and processing take place in facilities within European Union territory. This tier applies to general

administrative tasks with low national secrecy, and European branches of non-EU companies, including U.S. firms, can meet this criterion and participate in bidding if they possess data centers inside Europe. Approval is granted through self-certification, where the supplier declares compliance on its own, and no separate third-party audit is required.

Level 2 goes beyond where data is physically located to examine the software supply chain that handles that data. Suppliers must submit a Software Bill of Materials (SBOM) detailing software components and have their source code verified for security vulnerabilities. A Software Bill of Materials is an exhaustive list detailing which components—that is, which external libraries and open-source elements—make up a program. It is easy to understand if thought of as a concept similar to food ingredient labeling.

The intent is that when a security defect is discovered in any single component, users should be able to quickly check whether that defect exists in their system simply by reviewing the list. According to the BISI report, this tier is designed to apply to public services with a medium level of sensitivity, such as medical records or financial infrastructure. Even for non-EU companies, a pathway remains open to qualify for this level if they form a joint venture with a European enterprise to share ownership structure and demonstrate technical isolation mechanisms.

Starting from Level 3, the requirements become noticeably stricter. The headquarters of the supplying company and its subcontractors processing the data must actually reside within European Union territory, and controlling shares as well as board voting rights must be held by EU citizens. Key personnel maintaining the system must also be residents holding EU citizenship and pass background checks. However, according to the BISI report, the European Commission left an exception pathway in the proposal that partially relaxes these requirements for allied nations that have signed information-sharing treaties with the EU and have no judicial friction. This tier applies to tasks directly tied to security, such as national law enforcement investigation networks or terror threat analysis.

Which countries the allied nation exception will actually apply to has not yet been finalized. Countries that already maintain information-sharing treaties and judicial cooperation frameworks with the European Union are cited as candidates, but specific country lists were not disclosed at the proposal stage. This ambiguity is considered one of the items that will be most fiercely negotiated while CADA undergoes deliberation. Broadening the scope of the exception weakens the effectiveness of Level 3, while narrowing it requires enduring diplomatic friction with allied nations.

If it is hard to picture all four levels at once, think of access control in a building. Anyone with a visitor badge can enter the lobby, office floors require an employee ID, the server room can be accessed only by an approved few, and the innermost vault room is restricted to a select few who have passed background checks. The four levels of SEAL are structured similarly: as the sensitivity of the information increases, the scope of entities granted access grows narrower.

Level 4 is the stage with no exceptions. It applies to areas directly tied to national survival, such as defense, military secrets, and top-tier public order analysis. While maintaining the board nationality and staffing requirements of Level 3, it allows no exceptions even for allied nations. From system design to source code maintenance, it fundamentally blocks any room for foreign commercial capital to be involved. Suppliers must obtain the High grade, the highest tier in the European Cybersecurity Certification Scheme (EUCS) issued by the European Union Agency for Cybersecurity (ENISA), to participate in bidding. CADA did not create this EUCS certification scheme from scratch.

ENISA had been preparing this certification scheme for several years, but member states reportedly remained divided over whether to include a clause limiting non-European ownership stakes in the highest grade. Some member states, including France, strongly demanded ownership limits, while others opposed them, arguing that such restrictions would harm market competition. CADA's explicit inclusion of the EUCS High grade in Level 4 requirements is read as an attempt to lend legal weight to the ownership debate that had gone unresolved within the certification framework.

The BISI report also provided estimates on the proportions in which these four levels would apply in actual public procurement. Low-sensitivity general administrative tasks, which make up about 70 percent of all public technology adoption projects, are classified under Level 1. Moderate-sensitivity tasks, accounting for 20 percent, fall under Level 2. The remaining 10 percent is split between Level 3 and Level 4; the report projected that 9 percent would be assigned to Level 3 and 1 percent to Level 4. It is worth noting that these estimates are not finalized statistics but projections based on the report's analysis. Yet what these proportions indicate is clear.

The overwhelming majority of public procurement remains in Level 1 and Level 2, while Level 3 and Level 4, which demand complete European ownership, apply to only a tiny fraction of all projects.

This tiered design is not an entirely new invention. France already operates its own certification framework, SecNumCloud, requiring top-tier certification that fundamentally blocks the influence of the US CLOUD Act for the nation's highest-

security use cases. Managed by France's National Cybersecurity Agency (ANSSI), this certification requires cloud providers seeking the highest tier to hold a controlling stake owned by French or European Union capital. The BISI report assessed that CADA's four-tier structure expands the logic of this French certification system to the entire European Union level.

Because a system was already in place in France, CADA can be understood not as a completely novel experiment, but as a proposal to scale up a proven model.

Aside from France's SecNumCloud, several member states have developed their own certification schemes in their own ways. When standards vary by country, an inefficiency arises where a supplier certified in one country must undergo review from scratch for procurement in another. This is why CADA seeks to unify these standards under a single SEAL framework. If twenty-seven member states insist on different certification criteria, a sovereign cloud market spanning all of Europe can hardly take off in the first place.

The weight of the approval process also varies by level. Level 1 can be passed through self-certification by the supplier alone, with a simplified track that exempts small and medium-sized enterprises from duplicate paperwork reviews. In contrast, for Level 2 through Level 4, an independent third-party audit body designated by the European Union must meticulously verify even the system's original blueprints before specialized investigative agencies of member states grant final approval. An approval decision made by one member state is published to the common EU register and undergoes a 60-day mutual verification period during which other member states can raise objections. The proposed procedure dictates that if objections are not resolved within this period, the European Commission issues a final mediation plan to settle the dispute.

Allowing all twenty-seven member states to review a judgment made by a single country appears designed to prevent lax screening in one nation from becoming a loophole that lowers security standards across the entire Union.

Certification is not a one-time event. If a supplier's ownership structure or board composition changes, the very premise of its original SEAL rating can collapse. If a company certified as a European entity is later acquired by non-European capital, the question remains as to what happens to the status of the public contracts it was performing. The BISI report notes that CADA includes procedures for monitoring and re-evaluating such post-approval changes, but how frequently and how quickly those re-evaluations will take place has not yet been specified.

The question of who determines these levels also remains. Before putting a new project out for procurement, a public institution must first self-diagnose the sensitivity of the data handled by that project and determine which SEAL level applies. A project handling routine administrative documents is classified under Level 1, but even within the same agency, a project involving law enforcement or defense data can be placed in Level 3 or Level 4. If this determination is flawed, problems emerge down the road. If a contract is awarded under a lower level classification and it is later confirmed that the data is directly tied to national security, the institution is forced to dismantle and rewrite the existing contract.

The reason CADA's proposal seeks to establish both determination procedures and audit systems can be understood as an effort to reduce this risk of misclassification.

The compliance burden is not necessarily light even for large companies, but starting from Level 2, preparing a Software Bill of Materials (SBOM) and verifying source code require dedicated staff and capital. For emerging European cloud companies with limited capital, this burden can act as a barrier to market entry itself. Aside from CADA providing a simplified Level 1 track for small and medium-sized enterprises, unless support measures are established to help growing European firms scale up to higher levels, a paradox could arise where the market for higher levels opens only to a handful of well-capitalized conglomerates.

For this four-tier structure to work in practice, there are hurdles to overcome. Multiple industry reports commonly point out that domestic suppliers in the European market do not yet possess sufficient capacity to satisfy Level 3 and Level 4 requirements. The time required for European companies to meet these higher-tier requirements is not merely a matter of political will. Operating large-scale cloud services demands massive upfront investments in server hardware, networking, and cooling infrastructure, and recovering those investments requires securing a stable customer base over an extended period.

Major American cloud companies have already spent decades building this cycle of investment and return. Observers note that if European companies are to catch up with this cycle within a short period, the tier standards set by CADA alone will not be enough, and separate capital support for the companies meant to fill those tiers must move in tandem. No matter how meticulously the requirements are designed, if there is a shortage of companies capable of passing them, public institutions will ultimately retreat to lower-tier procurement or rely on exemption clauses. Rather than the tiers set by CADA themselves, how quickly the capabilities of European companies grow to fill

those tiers remains the variable determining the practical success or failure of this system.

Sources and References

1. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), July 7, 2026.

2. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

3. European Commission, SWD(2026) 502 final, Official Journal of the European Union, June 3, 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

4. European Commission, 'Cloud and AI Development Act', Shaping Europe's digital future, Official Journal of the European Union, June 3, 2026.

5. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, June 23, 2026.

6. Court of Justice of the European Union, Judgment in Case C-311/18 (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems), July 16, 2020.

4.3 The 'Sovereignty Termination Clause' and the Institutionalization of Portability Obligations

No matter how sophisticated a grading system CADA designs, if it fails to answer the question of how to terminate contracts that are already signed, that grading system remains a half-baked measure applicable only to new ventures. The case of the United Kingdom illustrates this issue most clearly.

In 2023, the UK's National Health Service (NHS) signed a £330 million contract with Palantir to build the Federated Data Platform (FDP). This platform is a system that aggregates and analyzes patient information, bed availability, and waiting lists from hospitals across the UK under a single framework. The Science and Technology Committee of the UK House of Commons issued a report warning that this contract posed an unacceptable national security vulnerability. Left-leaning outlet Novara Media reported that several MPs had demanded the government terminate the contract. The problem was that even if they wanted to terminate the contract, doing so was no easy matter.

According to the report by the House of Commons Science and Technology Committee, despite paying usage fees throughout the contract period, the NHS was unable to take ownership of the system's core assets—the Canonical Data Model and ontology intellectual property rights. The moment the contract ended, what remained in the hands of the NHS was not intact data, but data wreckage structured to operate exclusively on Palantir's software. The House report also confirmed that the termination for cause clause contained in this contract would not take effect until February 2027. There was a gap of several years between the moment they genuinely wanted to end the contract and the legal moment they could actually do so.

Public procurement contracts have always included termination clauses. Provisions allowing termination for breach of contract or termination for convenience, which incurs a penalty fee without requiring special cause, are commonly used. What CADA aims to introduce is a third category distinct from these two. Even if a vendor faithfully fulfills the contract, if the vendor's nationality and governance structure are deemed a threat to national security, a separate ground would be established to terminate the contract without incurring penalties. If such grounds are not defined with legal clarity, it leaves open the risk that the vendor could file a lawsuit, claiming the termination was arbitrary.

The problem highlighted by this case is not limited to a specific company like Palantir. Once a public institution begins entrusting its data to a particular software, that data is increasingly conditioned to hold meaning only within the proprietary structure of that software. Moving data to another system involves more than simply copying files. In many cases, the taxonomy and relational structure in which the data is housed—that is, the ontology itself—must be redesigned. An ontology can be thought of as a blueprint defining how different pieces of information relate to one another. For instance, the system of rules dictating how patients, hospital beds, and medical records connect falls under this concept.

Restructuring this rule system to fit another company's system requires new contracts, development personnel, and a substantial budget. Herein lies the paradox: procurement that appeared inexpensive in the early stages of a contract demands even greater costs than the original contract at the time of transition. This structural lock-in effect is commonly referred to in the industry as vendor lock-in.

The lock-in effect demonstrated by the NHS case is not limited to traditional databases. Procurement in the age of artificial intelligence encompasses not only data, but also models trained on that data, adjusted model parameters, and embeddings used for retrieval as targets for transfer. If a vendor stores these elements in proprietary formats, public institutions are left with nothing but an empty infrastructure once the contract ends, while the intelligence built atop it remains entirely in the vendor's hands. Experts point out that for CADA's portability obligations to take practical effect, detailed regulations must be put in place to include such AI-specific assets among the items subject to transfer.

The most common way to technically guarantee portability is to mandate the use of open standards. If contracts stipulate that data must be stored in open formats readable and writable across multiple systems rather than in proprietary formats accessible only to a specific vendor, migrating data to another system after the contract ends becomes relatively straightforward. However, adopting open standards does not automatically transfer system-specific designs like ontologies. Changing the vessel containing the data to an open format and transferring the knowledge structure stored within that vessel remain separate challenges.

The concept of portability was not entirely absent from European Union law. The EU Data Act (Regulation (EU) 2023/2854), adopted in 2023, already contains provisions addressing switching between cloud and edge computing services. This legislation established a phased reduction in switching fees charged when cloud users move from

one service provider to another, eliminating such fees altogether after a set deadline. Unlike CADA, the Data Act differs in that it is a law that has already taken effect.

The relationship between the two laws becomes clear when CADA is understood as an attempt to extend the portability principles of the Data Act to the far more sensitive realm of public procurement and under the far heavier standard of sovereignty. Where the Data Act sought to protect ordinary commercial cloud users from vendor lock-in, CADA aims to expand that shield to state institutions and public services.

This is precisely the point that the CADA proposal seeks to address. One of the policy objectives stated by the European Commission is that public institutions hold the right to terminate contracts for sovereignty reasons, while vendors bear the obligation to transfer data and configuration values in open and interoperable formats upon contract termination. The BISI report summarized that one of CADA's three pillars is the institutionalization of this portability obligation, intended to prevent public institutions from becoming trapped by a specific vendor and losing bargaining power. The exact title and article number under which this provision will appear in the final regulation will be determined after deliberation by the European Parliament and the Council of the European Union.

What can be confirmed at present is the fact that the Commission included provisions of this orientation in its proposal, not that an active norm is already in force.

While the specific nature of the transition support period mentioned in the proposal has yet to be finalized, inferences can be drawn from examples in other industries where similar systems are already in operation. Mobile number portability, which allows telecom users to switch providers while retaining their phone number, and bank account switching services, which transfer direct debit histories alongside account transfers, serve as prime examples. Applying this concept to public sector data portability would likely require procedures where the outgoing vendor and incoming vendor operate systems side by side for a given period, executing a phased handoff of data and operations.

For this system to function, two conditions must be met together. One is explicitly codifying the termination right in law, and the other is securing technical portability so that this right can actually be exercised. If only a legal provision exists while data formats remain closed, public institutions may have the right to end a contract, but they have no way to exercise that right. Conversely, even if data can be transferred technically, if penalty clauses are embedded in the contract, public institutions remain stuck in legacy systems due to immediate costs. The case of the NHS is a record of failure demonstrating what happens when neither of these two conditions is satisfied.

Even if CADA actually goes into effect, whether it will apply retroactively to existing contracts remains a separate issue. Generally, new EU regulations apply primarily to contracts entered into after the date of implementation, with grace periods or separate transitional provisions often attached for existing contracts. How transitional rules for existing contracts will be structured during the finalization of the CADA proposal is highly likely to become a central point of negotiation among member states. For public institutions that have entrusted their data to a specific vendor for many years, it could take a long time to feel the actual impact of portability obligations if the new regulations do not apply retroactively.

Such costs are hardly visible at the time of initial contracting. Procurement officers typically compare vendors based on initial adoption costs and annual service fees, and rarely calculate in advance the cost of extracting data after the contract ends. This asymmetry creates its own incentive for vendors. Numerous market analyses have pointed out that offering low initial pricing to win a contract and then locking customers in by raising switching costs is a common strategy in the cloud industry. CADA's portability obligation can be seen as an attempt to alter this incentive structure itself starting from the pre-contract stage.

This issue weighs more heavily on smaller countries than on larger ones. Member states with large populations and ample budgets can afford separate dedicated legal and technical teams to review contracts. In contrast, local governments or small public institutions in smaller member states often lack even sufficient specialized personnel to review contract documents. Accepting the vendor's standard contract as presented is more convenient in the short term than lingering over negotiations. As this asymmetry accumulates, even if the right of termination for cause exists in the statute books, a gap emerges between institutions that possess the capacity to exercise that right and those that do not.

Following a logic similar to how the CADA proposal opens a simplified approval pathway for small and medium-sized enterprise (SME) suppliers, observers note that preparing standardized portability requirements and contract templates in advance for contracting public institutions is the way to narrow the gap in bargaining power.

The problem of switching costs persists even after a contract ends. Separate from the work of transferring data, it requires time and budget for the staff members who handled that data to learn the new system. Because public institution budget cycles are typically structured on an annual basis, it is often difficult to secure all at once switching costs that are distributed over multiple years. For this reason, even where the right of termination for cause exists legally, cases have been reported across multiple

countries where budget departments could not absorb switching costs, effectively extending the contract. The effort in the CADA proposal to stipulate a transition support period alongside portability obligations appears to be a design crafted with these practical barriers in mind.

Codifying the right of termination for cause and portability obligations in law brings another legal tension. The European Union's Public Procurement Directive (Directive 2014/24/EU) and the World Trade Organization Agreement on Government Procurement (GPA), to which the European Union is a party, stipulate in principle that qualified foreign suppliers must not be unfairly discriminated against in procurement processes. While exceptions grounded in national security and defense rely on Article 346 of the Treaty on the Functioning of the European Union (TFEU), this exception was designed strictly as an exception, not as the rule.

If CADA effectively produces the outcome of excluding non-European companies from procurement at the higher levels of SEAL, legal disputes are likely to follow regarding whether that exclusion falls within the legitimate scope of the security exception. This tension remains an issue that will continue to be contested over the exact wording of every provision while CADA undergoes deliberation by the European Parliament and the Council of the European Union.

There is another figure that gauges the weight of this issue. In its second-quarter 2026 earnings release, Palantir announced that it recorded a year-over-year revenue growth rate of 93 percent. German media outlet Netzpolitik reported that even while European countries declared their intention to distance themselves from Palantir in law enforcement and defense, European investment banks and asset managers were channeling billions of euros into buying Palantir stock. This contradiction—pushing the firm out through the door of public procurement while sending capital through the window of financial markets—cannot be resolved by a single legal provision.

One must also not lose sight of the fact that portability obligations are a direction-neutral tool. Regulations making it easy to transfer data do not open pathways exclusively to European firms; they also open pathways to other American companies. The right of termination for cause and the portability obligation themselves are not mechanisms to favor firms of a specific nationality, but rather instruments that bolster the overall bargaining power of public institutions. For that bargaining power to actually result in selecting European companies, the nationality and governance requirements defined by the SEAL framework must ultimately operate alongside them.

A gap remains between declarations of defending sovereignty and the actual supply capacity of European alternative software to support those declarations. CADA's

termination rights and portability obligations are an institutional first step toward bridging this gap. Whether that first step works in actual procurement settings will become clear through the outcome of the European Parliament's deliberations and the subsequent implementation process.

Sources and References

1. UK House of Commons Science and Technology Committee, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', House of Commons, 2026.

2. Novara Media, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026.

3. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), July 7, 2026.

4. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, 2026.

5. Jan Ebert, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026.

6. European Union, Regulation (EU) 2023/2854 (Data Act), Official Journal of the European Union, 2023.

5.1 Francesca Bria's "EuroStack" Concept and the 300 Billion Euro Investment Barrier

Francesca Bria is an Italian economist who has served as an advisor to the European Commission. Serving as Commissioner for Digital Innovation at Barcelona City Hall, she led policies that enabled the city itself, rather than private corporations, to manage data generated by citizens. This background later became a frequently cited reference point as she designed digital policy at the European level. In numerous speeches and writings, Bria has voiced concern that handing public infrastructure over to American private tech companies could undermine the foundations of democracy.

The events covered in the earlier chapters of this book—namely, France's General Directorate for Internal Security (DGSI) moving away from Palantir or Anthropic blocking access—can be seen as concrete examples showing that this concern is not merely an abstract anxiety. The point Bria repeatedly emphasizes in designing EuroStack is also not the clauses of a contract, but the question of who owns and controls the infrastructure itself.

According to reporting by the investigative media outlet Follow the Money, Bria highlighted in a separate study titled "The Authoritarian Stack" how European investment banks and asset managers were funneling large amounts of capital into American companies like Palantir. She pointed out the contradiction of European pension funds and banks financing the very companies that encroach upon their own domestic public infrastructure. This critique connects directly to the flow of European internal investment capital discussed later in this section.

The blueprint translating these concerns into concrete form is the EuroStack report. Its official title is "EuroStack – A European Alternative for Digital Sovereignty," co-authored by Bria, Paul Timmers, and Fausto Gernone. The private German foundation Bertelsmann Stiftung published the report on February 13, 2025. Bertelsmann Stiftung is a non-profit foundation established by Bertelsmann, a major German media group, and has long sponsored research on European social and economic policy.

That this foundation published the EuroStack report means it is an independent proposal sponsored by a policy research foundation, not an official European Union document. This fact must be noted from the outset. EuroStack is not a law or policy adopted by the European Union. It is a policy proposal published by a private foundation, urging the European Union and member state governments to move in this direction. The figures and blueprints discussed in this chapter are all contained within

this proposal, and must be read separately from budgets currently being executed or regulations already enacted.

The Cloud and AI Development Act (CADA) covered in Chapter 4 and this report exist on different tiers. CADA is a proposal for a regulation submitted by the European Commission to the European Parliament and the Council of the European Union, currently going through formal legislative procedures. EuroStack, by contrast, is a policy report from a private foundation outside those procedures. While CADA addresses building data centers within Europe and determining the nationality of their operating companies, EuroStack is a vision to achieve self-reliance across all seven layers—from semiconductors to artificial intelligence—on a far broader scale.

While both documents share the common goal of European technological self-reliance, they carry different legal weight: one is a regulatory proposal undergoing the legislative process, while the other is a policy proposal setting out a direction from outside that process.

In explaining the EuroStack concept, Bria has drawn comparisons to the introduction of the euro, Europe's single currency. Just as Europe tore down currency barriers and established a shared financial order in an era when member states used different currencies, the point of this analogy is that capabilities scattered across member states must be consolidated in the digital infrastructure domain as well. Considering that introducing the euro required years of negotiations and treaty revisions, this analogy can be read as an effort to emphasize the vast scale of integration targeted by EuroStack.

The report divides Europe's digital foundation into seven layers. At the very bottom lie the raw materials needed to manufacture semiconductors and batteries, as well as the energy and water required to run data centers. Above that are stacked, in order, the layer for manufacturing semiconductor chips, the layer for deploying broadband telecommunications networks, the layer for manufacturing sensors and Internet of Things devices, and the layer for operating cloud infrastructure. At the top reside the software layer and the data and artificial intelligence layer. The report argues that if non-European companies hold even one of these seven layers, self-reliance for the remaining layers built on top of it can never be complete.

The logic is that even if semiconductors are manufactured domestically, if the servers containing those chips are run exclusively in data centers owned by American companies, self-reliance remains only half complete.

This seven-layer structure is easier to understand when compared to the process of building a house. No matter how sturdy the materials used to build the walls, if the roof placed on top must be bought according to someone else's blueprint, the safety of the entire house comes to depend on the person selling the roof. The self-reliance described in the EuroStack report is no different. The report's central argument is that even if European companies produce everything up to semiconductors, networks, and the cloud, relying on products from American companies for the artificial intelligence models and data management software running on top means the achievements in the bottom six layers can be undermined by that single top layer.

The report also proposes five shared services combining these seven layers to be provided directly to citizens: a sovereign cloud service processing computations within Europe, a digital identity wallet verifying citizen identities, a digital euro payment system enabling payments without bank fees, a federated data space securely exchanging data among member states, and an artificial intelligence engine designed and operated directly by Europe. All five are areas currently dependent on services from American or other non-European companies, and the report explains that removing this dependence is the practical objective of the EuroStack concept.

Among the five services, the one closest to citizens' daily lives is the digital euro payment system. Currently, when a payment is made by card in Europe, the transaction data usually passes through the processing network of an American card company. A significant portion of the fees merchants pay every time they accept card payments flows to the company owning that payment network. The digital euro system proposed by the report is a concept aimed at bringing this payment network itself under the European Central Bank system, ensuring transaction data does not leave the region while also altering the fee structure. The digital identity wallet stems from a similar concern.

The idea is to establish a state-managed means of identity verification rather than relying on current practices where citizens verify their identity online through single sign-on systems of specific Big Tech companies. It is also worth noting that among these five services, the digital identity wallet is not a concept proposed for the first time by the EuroStack report. The European Union had already adopted the European Digital Identity Regulation—the so-called eIDAS 2.0—in 2024, requiring member states to provide an EU Digital Identity Wallet to citizens. This regulation is a law already enacted and in effect, separate from the EuroStack report.

Rather than proposing to scrap this existing system and build a new one, the EuroStack report leans toward proposing that this ongoing movement be incorporated into a

seven-layer structure and organically linked to the other layers. The remaining three services correspond closely to the layer facing governments and companies. The sovereign cloud service overlaps in its goals with the sovereignty assurance level system of CADA discussed in Chapter 4.

Unlike the so-called sovereign cloud products offered by Amazon Web Services or Microsoft for European customers, which carried the limitation of not transferring controlling stakes to Europe as examined in Chapter 4, the sovereign cloud service envisioned by EuroStack refers to a cloud whose ownership itself resides in Europe. The federated data space is a conduit ensuring that member state governments and companies do not route through American clouds when exchanging data. This initiative is also connected to the Gaia-X project launched by France and Germany in 2019, which predates CADA covered in Chapter 4.

While Gaia-X was evaluated as having ended up merely as a voluntary standardization attempt without legal binding force, the EuroStack report proposes elevating this data-sharing system into a shared infrastructure backed by state budgets. The sovereign artificial intelligence engine embodies the goal of altering the current situation in which European public institutions and companies rely on large language models developed by American or other non-European companies.

The scale of investment proposed by the report is not small. The authors estimated that building this seven-layer infrastructure anew would take roughly ten years, stating that a total capital of 300 billion euros would be required by 2035. Additionally, it included a proposal to create a separate tech fund worth 10 billion euros to serve as seed money. Dividing 300 billion euros over ten years means that an average investment of 30 billion euros per year must be maintained continuously. This figure is the calculation of the report's authors and is not an officially adopted or allocated budget of the European Union.

Placing this sum side by side with the budget that the European Union actually operates reveals a gap. A report published in September 2025 by CERRE, a policy research institute, stated that the budget allocated to digital sovereignty items within the Competitiveness Fund pursued by the European Union was around 55 billion euros. Compared to the 300 billion euros demanded by the EuroStack report, this is less than a fifth of that size. The Competitiveness Fund is a budget item the European Union intends to organize under the next multiannual financial framework starting in 2028 to boost digital and industrial competitiveness, and it has yet to receive final approval from member states and the European Parliament.

This implies that even this budget is not a finalized amount, and within it, the share allocated to digital sovereignty falls far short of the amount demanded by EuroStack. The meaning of this comparison is clear: EuroStack is a blueprint indicating a direction, not a sign that the budget to complete that blueprint has already been secured.

European policy debate participants, including Bria, point to private savings rather than government budgets to fill this funding gap. According to a report by the media outlet EU Perspectives in January 2026, total household bank deposits in the European Union exceeded 30 trillion euros as of 2026. According to figures mentioned in a debate hosted at the World Economic Forum's annual meeting in January 2026, this amount is more than double the total gross domestic product of the entire European Union. The problem is that this money is not moving.

According to contents mentioned in a discussion covered by the European edition of Politico on June 4, 2026, while there are countries like Sweden where more than half of citizens put money into stocks or funds, that proportion remains around 2 percent in several large European member states. Money locked up in banks fails to flow into startups, and the discussion pointed out that a significant portion of the money that actually goes into investments flows toward major U.S. tech stocks.

Pension funds face a similar problem. According to points raised in a panel discussion broadcast by France 24 in June 2026, European pension funds are bound by supervisory regulations that prioritize stability, making it difficult to finance tech companies in early growth stages. Regulations such as Solvency II, the European Union's insurance and pension supervision framework, require pension funds to maintain a certain proportion of safe assets to prevent sudden losses.

Although the intent of this regulation is to safeguard retirees' funds, it consequently narrows the path for pension funds to flow into assets with high risks and uncertain returns, such as early-stage tech companies. This capital bottleneck also leads to a brain drain. The trend of European technical talent moving to Silicon Valley in the United States after failing to secure funding was mentioned in the same discussion. The accompanying staff working document SWD(2026) 502 final, released by the European Commission along with the CADA proposal, demonstrates this funding gap numerically.

Europe accounts for merely 5 percent of global venture capital investment, whereas the United States accounts for 52 percent. In a 2024 CEPS lecture, Bria pointed out that a significant number of successful startups born in Europe are acquired by foreign capital when they reach the scaling phase and move outside Europe.

Based on this diagnosis, Bria has demanded tax reforms that encourage bank deposits and pension assets to flow into European technology companies. Mentioned methods include granting tax cuts to citizens who invest in domestic tech firms instead of keeping savings locked away long-term, or raising the limits on pension funds' investments in risk assets. Whether such proposals have led to actual legislation remains unconfirmed within the scope of materials examined in this book. The logic of the report is that if a significant portion of the 300 billion euros demanded by the EuroStack report is to be filled by private capital rather than state budgets, such tax reforms must come first.

This is not to say that capital is not moving at all. According to a June 4, 2026 report by the French-language financial outlet EcoQuick, the European Union finalized a plan to inject 20 billion euros in public funds into constructing artificial intelligence Gigafactories. In a July 1, 2026 announcement, the Spanish Prime Minister's Office stated that it approved an agreement to invest 720 million euros of public budget to construct an artificial intelligence Gigafactory in Spain. Startup Online reported on May 21, 2026, that the 5 billion euro Scaleup Europe Fund, managed by the Swedish asset management firm EQT, is also scheduled to start disbursing funds in the fall of 2026.

This fund operates in conjunction with a 1 billion euro deep-tech fund created by KfW, the German development bank.

Even when combining all these actually committed amounts—20 billion plus 720 million plus 5 billion—the sum falls short of 30 billion euros. This is barely a tenth of the 300 billion euros requested by the EuroStack report. While it is true that the European Union and several member states have actually opened their wallets, the scale remains far short of filling the blueprint presented by Bria.

Placing these numbers side by side makes the nature of the problem clearer. European Union household bank deposits top 30 trillion euros, while the investment required by the EuroStack report is 300 billion euros. In pure arithmetic terms, moving just 1 percent of these deposits into technology investment would cover the entire amount called for in the report. The problem is that the incentives and systems needed to mobilize this 1 percent are not yet in place. The essence of this gap is not a lack of money, but a shortage of tax incentives, financial products, and trust to shift funds from savings into investment.

Unless this gap narrows, many of the seven layers envisioned by EuroStack will remain on the drawing board. Layers that require massive upfront investment, such as semiconductors and data centers, feel the impact of this funding shortfall first. This is why critics point out that allocating budgets member state by member state cannot

support a project worth 300 billion euros, and why Bria seeks to draw in private savings and pension assets.

How much the European Union expands its digital sovereignty budget in the upcoming budget negotiations starting in 2028 will serve as the next test of whether the EuroStack initiative can move from blueprint to actual project. Until the outcome of those negotiations emerges, EuroStack remains a map pointing in the direction Europe wants to go, not a finished building.

Sources and References

1. Francesca Bria, Paul Timmers, Fausto Gernone, 'EuroStack – A European Alternative for Digital Sovereignty', Bertelsmann Stiftung, February 13, 2025, https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty

2. Johanna Bröer et al., 'Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?', CERRE Issue Paper, September 2025, p. 17.

3. Joana Soares, 'Your cloud data lives on American servers. Brussels is moving to act', EU Perspectives, January 2026.

4. World Economic Forum, 'Is Europe's Tech Sovereignty Feasible?', WEF Annual Meeting 2026, January 2026.

5. POLITICO Europe, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, June 4, 2026, https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/

6. FRANCE 24 English, 'Can Europe own its digital destiny? EU unveils tech sovereignty roadmap', FRANCE 24, June 2026.

7. European Commission, SWD(2026) 502 final, Official Journal of the European Union, June 3, 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

8. Francesca Bria, 'EuroStack: a concrete pathway to European digital sovereignty and strategic autonomy', CEPS Think Tank, 2024.

9. Loïc Kraft, 'Souveraineté numérique : Bruxelles renâcle à imposer des contraintes trop fortes', Echo Quick, June 4, 2026.

10. Presidency of the Government of Spain, 'The President calls for public-private partnership to drive forward Spain's artificial intelligence gigafactory', La Moncloa, July 1, 2026.

11. Editorial Board of Startup Online, 'Research Report on Computing Power, Cloud, Open Source, and Capital for European Digital Sovereignty (Yureop dijiteol jugwoneul wihan yeonsanryeok·keullaudeu·opeonsoseu·jabone gwanhan yeongu bodo)', Startup Online, May 21, 2026.

5.2 Alternative Software Alliance: Arcadia and Open-Source Digital Public Goods

Command and control systems, software often abbreviated as C2, are tools that aggregate what is happening on the battlefield onto a screen and convey commanders' orders to units. They organize and display in real time which units are where, what targets have been discovered, and which orders have been issued to which units. If the Maven Smart System covered in Chapter 3 fulfills this role at the NATO alliance level, Arcadia is France's attempt to replace that same role with its domestic software.

France is developing a nationally led military artificial intelligence command and control system to replace Palantir's Maven Smart System. Its name is Arcadia. According to a joint report published on July 9, 2026, by defense media outlet Armees.com and Économie Matin, Arcadia is battlefield command software being developed by a consortium comprising Thales, Airbus, Safran, and French large language model developer Mistral AI. Tactical software startups such as Command AI and Impact have also joined the effort.

Mistral AI is a large language model developer founded in Paris in 2023, widely considered to hold the leading position among artificial intelligence companies originating in Europe. The fact that this company joined a military consortium demonstrates that Europe's civilian artificial intelligence industry is combining with the defense domain.

Arcadia is not a project that started from scratch. According to the same report, France had previously pursued the SIA C2 combat command post system, a joint effort between Thales and Sopra Steria, for several years, but experienced the project's cancellation due to technical incompatibility issues. Learning from this failure, the Arcadia consortium designed the system from the beginning to be modular. By applying open application programming interfaces (APIs), they allowed software components made by different companies to integrate with one another, while also satisfying NATO's Federated Mission Networking (FMN) standards, which support wireless communications among allied forces.

FMN is a set of common specifications established so that different command and control systems of NATO member states can exchange information during coalition operations. The purpose of this standard is to enable target information identified by one country's units using their domestic system to be read in the same format by another country's system that follows FMN standards. That Arcadia meets this standard

means France has not given up its ability to share information with allied forces even while using independent software. It is a design intended to satisfy both national design sovereignty and interoperability with allied forces at the same time.

Modular design is an approach in which standardized components are purchased from multiple companies and assembled, rather than buying a single large finished product whole. Even if the company that built one component closes down or terminates its contract, replacing it with another company's component that meets the same specifications allows the overall system to continue operating. Unlike the previous SIA C2 project, which was held back by a specific vendor's proprietary design, Arcadia uses this modular structure to reduce the risk of the entire system being dictated by the circumstances of a single firm.

CWIX is a regular NATO event standing for Coalition Warrior Interoperability Exercise, a venue where member states annually check whether their developed weapon systems and communications equipment can actually interface with one another. Testing whether newly developed command and control software can actually communicate with other allied equipment during this exercise has become standard practice. Arcadia was pilot-tested for the first time at this exercise held in Bydgoszcz, Poland, in June 2026. According to a report by defense news outlet Defense News on June 5, 2026, this exercise served to verify Arcadia's ability to process data in an operational environment.

This means that rather than fully deploying a completed system to actual combat, it was a stage of testing a system under development against NATO standards. According to the same report, General Patrick Justel, deputy chief of staff of the French Army, remarked during the exercise that accepting foreign software without verification amounts to surrendering national sovereignty, explaining that Arcadia is France's response to American military technological superiority.

There is a clear difference between the development approaches of Arcadia and Maven. Palantir adopted a single-vendor model, developing the Maven Smart System as proprietary software and supplying it to NATO. Arcadia, by contrast, adopted a consortium model in which Thales, Airbus, Safran, Mistral AI, and several startups each build their respective domain expertise in modular form and combine them. It is a design intended to prevent any single company from dictating the entire system. While this approach has the drawback of potentially slowing development, it offers the advantage of reducing the risk of relying on a single firm for an entire security infrastructure.

This trend is not limited to France. According to a report by media outlet The Next Web on July 18, 2026, the French and German governments jointly pledged to build a European-level competitive system to counter Palantir's military artificial intelligence software. Whether this pledge led to concrete joint development plans or remained confined to each nation pursuing independent projects like Arcadia is unclear from the materials verified in this book. According to a list compiled in April 2026 by consulting firm Pathfinders Group, there are several other companies cited as alternatives to Palantir within Europe beyond the participants in the Arcadia consortium.

This means a structure is taking shape in which multiple companies compete in their respective areas rather than a single winner being decided.

Arcadia remains a French-led project to date, and most companies participating in the consortium are French firms. Although the CWIX exercise was a multinational event involving NATO member states, Arcadia itself has not been adopted as an official standard for all of NATO. Whether member states outside France will actually adopt this system or whether each country will use a separate system developed domestically is not yet settled within the scope of materials verified in this book. If European nations develop separate command and control systems individually, interoperability among European countries could emerge as a new challenge this time around.

Safran's role in this consortium warrants separate examination. According to a report by French financial media outlet L'Essentiel de l'Économie on June 8, 2026, Safran, which started as an aircraft engine manufacturer, has acquired a succession of intelligence analytics firms since 2022. In July 2022, it acquired Orolia—which provides precise positioning signals even in jammed environments—for $101 million, and in 2024 absorbed satellite imagery analytics firm Preligens for €220 million to launch its new Safran.AI division. In February 2026, it acquired Syntony, which possesses anti-jamming technology for underground spaces, and in May 2026 additionally acquired the defense division of radar imagery analytics firm Kairos.

According to the same report, the Safran.AI division employs 300 engineers, saw its 2025 revenue increase by 65 percent year-over-year, and expects 90 percent growth in 2026. The outlet reported that the target recognition engine ACE developed by this division is also being used to enter joint development agreements with partners in Singapore, Canada, and India. The significance of this list of partner countries is also worth noting. Singapore and India are countries that do not belong to Five Eyes, the US-led intelligence-sharing alliance, yet have maintained security cooperation with the West.

Safran's partnership with these countries can be read as an attempt to expand a separate intelligence cooperation network outside the US-centric intelligence alliance. This example of a company that once built aircraft engines acquiring a series of intelligence analysis firms over a few years to transform into an artificial intelligence firm also illustrates how European defense conglomerates are rapidly acquiring software and data capabilities through acquisitions rather than developing them in-house.

Outside the military domain, a movement centered on open-source software is under way. Document COM(2026) 503 final, published in the official journal by the European Commission on June 3, 2026, estimated that European Union member states pay 264 billion euros annually in subscription fees for American software. To reduce these costs, the same document outlined an open-source strategy based on the principle of making the source code of software built with public funds available to citizens free of charge, the so-called "public money, public code" principle.

The reason these costs recur lies in the lock-in effect peculiar to the software industry. Once a government agency begins creating and storing documents with a specific company's office software, trying to move to another vendor's product after several years causes switching costs to balloon because document formats and work procedures have already been tailored to that company's system. Because the burden of these switching costs outweighs the annual subscription fee, agencies choose to renew their contracts. It is this lock-in structure itself that the open-source strategy targets.

The logic is that making source code public so that multiple companies compete on the same codebase prevents getting tied to a single vendor.

In accordance with this principle, the governments of France, Germany, Italy, and the Netherlands formed a European Digital Infrastructure Consortium named Digital Commons EDIC in October 2025. EDIC, short for European Digital Infrastructure Consortium, is a legal structure used when multiple member states undertake joint projects. Instead of each government entering separate contracts, this single entity pools budgets and manages projects on behalf of participating countries. At the center of this consortium is openDesk, an office collaboration software suite approved for development by Germany's Federal Ministry of the Interior as an alternative to Microsoft 365.

openDesk is a software suite that bundles together the file storage tool Nextcloud, the mail server Open-Xchange, the content management tool Drupal, and the decentralized messenger Matrix. Instead of each local government modifying the source code separately, they manage it together through a shared repository called openCode.

According to the German procurement outlet Cosinex Blog, this open-source strategy is pursued alongside an administrative principle known as "Once-Only." Once-Only is a principle under which government agencies share information already submitted by citizens or businesses so they do not have to resubmit documents or data to multiple agencies.

openCode, which shares source code, and Once-Only, which shares administrative data, handle different objects, but both stem from the same idea of reducing duplication and sharing resources. Related reports state that France's collaboration software La Suite, Germany's openDesk, and the Netherlands' MijnBureau actually demonstrated that software from three different countries could exchange documents without passing through foreign clouds. The implications of this demonstration are significant. Until now, civil servants from different countries often ended up converging on the same American cloud accounts to exchange documents.

Showing that three countries could interoperate while using different software means European nations have a way to achieve interoperability without standardizing on a single software product.

This open-source strategy is expected to dovetail with CADA's Sovereign Assurance Level framework discussed in Chapter 4. General administrative software like openDesk or La Suite will likely fall into lower, less sensitive tiers under the SEAL framework, while software directly tied to national defense like Arcadia will likely face strict requirements at higher tiers. How open-source software and the SEAL grading system fit together in practice will be clarified as CADA finalizes its text.

There are also examples at the local government level. According to data compiled by the European Commission's Interoperable Europe Portal, the northern German state of Schleswig-Holstein began removing Microsoft operating systems and Outlook from 25,000 civil service computers in 2020 to transition to LibreOffice. A press release issued by the state government on December 4, 2025, noted that this transition saved the state 15 million euros annually in software licensing costs.

Switzerland went further by enacting legislation. As reported by the Swiss news outlet Watson on December 4, 2024, Switzerland passed the Federal Act on the Use of Electronic Means for the Fulfillment of Authorities' Tasks (EMBAG) in 2024, requiring as a matter of principle that source code for all software built with public funds be released as open source. Under this law, the Cyber Command of the Swiss Armed Forces General Staff released its internally developed security analysis software, Loom, to the public free of charge. Given that military releases of in-house software as open source

are rare, this decision illustrates how far Switzerland is willing to push its technological self-reliance.

This trend stems from the same root as the transition to ArgonOS by France's General Directorate for Internal Security (DGSI) and the departure from Palantir by Germany's Federal Office for the Protection of the Constitution (BfV), both examined in Chapter 1. While Chapter 1 addressed domestic intelligence agencies' decisions to move work previously handled by Palantir to other vendors' products, Arcadia and openDesk, discussed in this section, are development initiatives aimed at creating those replacements within Europe itself. Deciding to change procurement sources and creating the product that allows for such a change represent challenges at different levels.

Arcadia, openDesk, and EMBAG operate on different levels. Arcadia addresses military command and control software, openDesk handles office software for public administration, and EMBAG codifies the obligation to release source code into law. The three share a single core principle: choosing to build software inside Europe whose source code can be owned and modified, rather than renting commercial products from foreign corporations.

It remains to be seen how widely this judgment will spread. While there are cases that have produced noticeable results, such as Schleswig-Holstein or the Swiss Armed Forces, not all European Union member states are moving toward open-source transition at the same pace. The more deeply a government agency is already entangled in Microsoft or Google software, the greater the initial transition costs and employee retraining burdens, and the political will to take on these burdens is not formed to the same degree across all member states. What Arcadia and openDesk have shown is potential, not a completed transition across Europe.

Sources and References

1. Jean-Baptiste Le Roux, 'Cloud de combat : face à Palantir, la France veut faire émerger un champion national des logiciels militaires', Economie Matin, July 9, 2026.

2. Jean-Baptiste Leroux, 'IA de combat : face au Palantir, la France veut son Maven hexagonal', Armees.com, July 9, 2026.

3. Rudy Ruitenberg, 'France to test its own AI-powered battlefield command in June NATO exercise', Defense News, June 5, 2026.

4. L'Essentiel de l'Éco Editorial Department, 'Comment Safran devient un géant du renseignement par IA', L'Essentiel de l'Éco, June 8, 2026.

5. European Commission, COM(2026) 503 final, Official Journal of the European Union, June 3, 2026, https://ec.europa.eu/newsroom/dae/redirection/document/129100

6. Digital Independence Editorial, 'Digital Sovereignty in Europe', Digital Independence, February 16, 2026.

7. European Commission, 'Open source progress in Schleswig-Holstein', Interoperable Europe Portal, 2026.

8. State Government of Schleswig-Holstein, Press Release, December 4, 2025.

9. Watson Editorial Department, 'Schweizer Armee setzt auf europäische Software statt Microsoft', Watson, December 4, 2024.

10. TNW Editorial Department, 'France and Germany pledge to build a European rival to Palantir's military AI software', The Next Web, July 18, 2026.

11. Pathfounders Group, 'Here are the top five companies vying to take on Palantir in Europe', Pathfounders Group, April 2026.

12. Wolf Witte, 'Vergabebeschleunigungsgesetz und digitale Souveränität 2026', cosinex Blog, May 21, 2026.

5.3 Economic Sovereignty Against Tax-Avoiding Multinational Corporations: The CICTAR Report and Protecting Public Finances

European governments pay substantial procurement budgets every year to American companies such as Palantir. A report examining how much of this expenditure returns to European society in taxes was released on August 5, 2026. The Center for International Corporate Tax Accountability and Research (CICTAR) is a research organization that tracks the tax avoidance structures of multinational corporations; prior to Palantir, it had published reports analyzing the tax practices of various multinational firms. This time, it narrowed its focus to Palantir.

Prepared with support from the European Federation of Public Service Unions (EPSU), the report analyzed Palantir's tax structure and argued that the company pays very little tax relative to the profits it earns from public contracts. This content was summarized and reported in an article by the investigative media outlet Follow the Money on August 5, 2026. EPSU is a European-level trade union federation representing public sector workers. Because the trend of private companies, including Palantir, increasing public procurement directly affects public sector jobs and budgets, it is worth noting that EPSU's funding of this investigation represents support from an interested party.

While this fact does not automatically invalidate the report's analysis, it is useful context for readers when evaluating the report.

Behind the report's coverage of the German case lie actual police procurement contracts. According to German media outlet Labanet Germany, police in several German states, including Hesse, have used Palantir's software to track and analyze potential threats—referred to in German as Gefährder. The report explains that the accumulation of such contracts across multiple states served as the background for the scale of tax revenue loss in Germany estimated by CICTAR.

The effective tax rate is the actual tax paid by a company divided by its pre-tax profit. No matter how high the statutory tax rate may be, if the actual tax paid decreases through various deductions and accounting techniques, the effective tax rate drops accordingly. What the CICTAR report takes issue with is not that Palantir broke the law, but that it used layers of legitimate accounting techniques to lower this effective tax rate. Tax evasion, which violates tax laws, and tax avoidance, which reduces taxes within the framework permitted by tax laws, fall into legally distinct categories. What

this report accuses the company of is the latter. This distinction also affects how the issue is addressed.

While tax evasion is subject to investigation and punishment, tax avoidance cannot be prevented by penalizing individual corporations. This means that institutional responses—such as amending tax laws themselves, restructuring bilateral tax treaties between countries, or changing the conditions of procurement contracts—are required. The Business in Europe: Framework for Income Taxation (BEFIT) proposal and the demands for revising procurement specifications, which will be discussed later in this chapter, represent precisely these types of institutional responses.

The CICTAR report claims that Palantir's global effective corporate tax rate for 2025 was just 1.4 percent. According to the report, Palantir earned approximately $1.66 billion in pre-tax profits in 2025 alone, but paid only $22.7 million in corporate taxes worldwide. These figures are based on analysis by CICTAR and Follow the Money, and this book has not independently verified Palantir's original financial statements. Nevertheless, the issue highlighted by this claim is worth examining.

Led by the Organisation for Economic Co-operation and Development (OECD) and joined by over 140 countries, this agreement is known as Pillar Two; after a broad agreement was reached in 2021, it has been sequentially incorporated into the domestic laws of participating countries. The goal of this agreement is to levy a corporate tax of at least 15 percent on multinational corporations regardless of where they operate. If the 1.4 percent figure presented in the CICTAR report is accurate, it is a result that departs significantly from the intent of this international agreement.

A separate report released on March 22, 2026, by the Institute on Taxation and Economic Policy (ITEP), a US tax policy research institute, analyzed that Palantir pays virtually no federal corporate income tax in the United States by utilizing immediate deductions for research and development expenses under tax incentive laws enacted during the Trump administration.

The CICTAR report also introduces the accounting techniques used by Palantir. Between the headquarters of a multinational corporation and its overseas branches, transactions commonly involve transfer pricing. This refers to transactions in which a branch sends money to headquarters under the name of technology licensing fees or service fees. Depending on how this amount is set, the branch's book profits vary greatly. If a branch sends a large sum of money to headquarters, the branch's profits decrease, and the corporate tax it owes to the country where it is located decreases accordingly. According to the report, Palantir's subsidiaries in European countries structure their accounting

books so that revenue generated from contracts is remitted to the US headquarters, receiving only a small service fee from the US headquarters in return.

Under this structure, the book profits of European subsidiaries are recorded lower than their actual scale of operations. In Spain, a different method was used, according to the report. The Spanish subsidiary remitted 70 percent of the profits earned from public procurement to the US headquarters as technology licensing fees, significantly reducing the taxable profit of the Spanish branch. Additionally, the report points out that stock-based compensation, which awards employees company shares instead of cash, is also treated as a tax-deductible expense to reduce taxable income. When a company distributes shares to employees, it can record the value of those shares as labor costs on its accounting books.

Since labor costs are recognized as expenses under tax law, as these expenses increase, taxable profits decrease. In the tech industry, where the practice of granting stock instead of paying salaries in cash is widespread, this method is commonly used as a legitimate means of tax savings.

The report also provides country-specific figures. CICTAR estimated that the tax revenue loss in Germany in 2024 due to this accounting structure reached 1.6 million euros, while the corporate tax actually paid by Palantir's German subsidiary that same year was only 640,000 euros. In Spain, the report notes that although Palantir signed a 16.5 million euro contract with national security agencies, the corporate tax it actually paid amounted to a mere 147,000 euros. All of these figures were analyzed and presented by CICTAR and do not represent official statistics released by the respective governments.

A separate case is confirmed in the United Kingdom. According to a report by media outlet Novara Media on June 4, 2026, the UK National Health Service (NHS) signed a 330 million pound integrated data platform contract with Palantir. This contract is referred to as the Federated Data Platform, a project aiming to integrate hospital and medical records across England into a single system. Palantir was selected as the preferred bidder for this project in 2023, sparking controversy in the British medical community and political circles from the moment of selection due to the contract handling sensitive patient health information.

According to the same report, Palantir's UK subsidiary paid only 2 million pounds in corporate tax to the UK tax authorities in 2024. Compared with the contract size of 330 million pounds, the corporate tax paid is less than one-165th of that amount. Of course, directly comparing the total contract value with a single year's corporate tax payment is not an accurate accounting method. This is because not all of the contract funds are

recorded as profit for that year, and corporate tax is levied on profit, not revenue. However, these figures show that the gap is strikingly large.

In a separate report, the UK House of Commons Science, Innovation and Technology Committee evaluated Palantir's growing presence in the public sector as an unacceptable vulnerability.

Placing the cases of Germany, Spain, and the United Kingdom side by side reveals a common pattern. All three countries entered into substantial public contracts with Palantir, but the corporate taxes actually collected were significantly small compared to the scale of the contracts. The CICTAR report analyzes that the fact that the results were similar even though tax authorities in the three countries examined the accounting in different ways suggests this accounting structure may stem not from lax oversight by a specific country, but from accounting policies that Palantir applies across multiple countries in common.

The country cited by the CICTAR report as an exception is France. According to the report, France's Directorate General of Public Finances (DGFiP) required Palantir to record profits earned within France entirely on the books of its French branch, and as a result, Palantir's French branch paid 1.6 million euros in corporate tax in 2024 at an effective tax rate of 33 percent. Compared to figures from other countries, this is a much higher proportion. The report interprets this difference as stemming from proactive tax enforcement by France's Directorate General of Public Finances (DGFiP). France is also a country that has levied a separate digital services tax since 2019 on large digital companies generating revenue within its borders.

This tax system targeting large US tech companies has caused trade friction with the US government on several occasions. The enforcement approach of France's Directorate General of Public Finances (DGFiP) regarding Palantir can also be viewed as an extension of this tax policy.

Rather than relying solely on tax enforcement by individual member states, the European Commission is separately pursuing a measure to harmonize the tax base of multinational corporations itself. This proposal, known as BEFIT (Business in Europe: Framework for Income Taxation), contains a provision requiring multinational corporations operating within the European Union to calculate taxable income based on a single common standard, rather than calculating taxes differently in each member state. This proposal is also still undergoing deliberation by the European Parliament and the Council of the European Union, and is cited as one of the attempts to fundamentally reduce the issue of profit shifting using transfer pricing, as highlighted in the CICTAR report.

Following the release of this report, reactions from organized labor followed. According to a report by the German media outlet Labnet Germany on August 5, 2026, Jan Willem Goudriaan, General Secretary of Public Services International (PSI), stated that the practice of entrusting critical national procurement to foreign suppliers that fail to protect public health and safety net budgets must stop. The same report also quoted a representative from FNV, the Netherlands' largest trade union, saying that the corporate practice of enjoying the benefits of public infrastructure while failing to pay corresponding taxes can no longer be tolerated. Organizations issuing such reactions are proposing that tax payment histories be incorporated into public procurement bidding specifications.

Until now, public procurement has used price and technical performance as the primary evaluation criteria, and the idea is to add how much tax the company actually paid to those criteria. Whether this proposal has been reflected in actual procurement regulations cannot be confirmed within the scope of the materials verified by this book.

This tax issue is also connected to the investment gap examined in Section 5.1. The Eurostack report estimated that Europe needs to raise 300 billion euros by 2035, and the budget actually allocated by the European Union fell far short of that. Those demanding tax reform argue that if non-European companies, including Palantir, had paid taxes commensurate with the profits they earned in Europe, as argued in the CICTAR report, that tax revenue could have formed part of the investment funds required by Eurostack. Of course, this causal relationship is a political argument advanced by supporters of the CICTAR report, not a fact independently verified by this book.

This tax issue leads to the same conclusion on a different level from the security issues discussed in previous chapters. Chapters 1 and 4 dealt with the issue of control that arises when entrusting national data and system operations to companies like Palantir. What the CICTAR report raises is the question of how much money actually returns to national finances from those contracts. Italy's National Cybersecurity Agency (ACN) stated that it set its policy toward excluding US-based platforms from critical national procurement by considering these two issues together.

The fact that two distinct grounds—taxation and security—point to the same conclusion is cited as the reason why European policymakers cannot postpone this issue.

The 300 billion euros demanded by Eurostack, the cost of developing Arcadia and Offendesk, and the tax bases highlighted by CICTAR ultimately converge on a single question: When Europe seeks to build a technological foundation independent of American companies, where will the money to build that foundation come from? Whether by unlocking deposits trapped in banks, developing software with already

secured budgets, or plugging leaking tax revenues, all three paths lead toward the same destination.

From the perspective of citizens, this issue is not an abstract accounting debate. Procurement budgets spent by police departments, hospitals, and the defense ministry come from taxpayers' money. If a significant portion of that budget does not return to the national treasury through taxes paid by contracting companies, the resources available for public services decrease accordingly. The core of the problem raised by CICTAR and Follow the Money is that this circular structure is currently broken. For the cycle—in which taxes are paid, public services are operated with those taxes, and those public services in turn support corporate activity—to function properly, the premise must hold that companies entering into procurement contracts pay their fair share of taxes in that country.

Sources and References

1. Sebastiaan Brommersma, 'Tech giant Palantir accused of aggressive tax avoidance at Europe's expense', Follow the Money, August 5, 2026, https://www.ftm.eu/articles/us-tech-giant-palantir-tax-avoidance-europe

2. Rika Baack, 'Dubiose Praktiken: Palantir drückt sich vor Steuern', netzpolitik.org, August 5, 2026, https://netzpolitik.org/2026/dubiose-praktiken-palantir-drueckt-sich-vor-steuern/

3. Rika Baack, 'Big Data bei der Polizei', LabourNet Germany, August 5, 2026.

4. ITEP, 'Palantir Pays Zero Federal Income Tax Despite Explosive Growth, Largely Due to Trump Tax Law', ITEP Reports, March 22, 2026.

5. Joshua Carroll, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, June 4, 2026.

6. UK House of Commons Science and Technology Committee, report, House of Commons, 2026.

7. Italian National Cybersecurity Agency, 'Sovranità digitale e IA: l'Italia tra autonomia e dipendenza', Italian Government, 2026.

Conclusion 1: Declarations Before Alternatives Mature, Overcoming the 2- to 3-Year Risk Interval

On December 15, 2025, Palantir announced that it had signed a new three-year multiyear contract with France's General Directorate for Internal Security (DGSI). Less than six months after this contract was signed, on June 16, 2026, French Prime Minister Sébastien Lecornu declared that the counterparty to this contract would be switched to the French company Hapsvision. The next day, Le Monde reported that Palantir claimed the renewed contract remained legally valid. An announcement and the termination of a contract are not the same event. This case, covered in Chapter 1 of this book, concisely illustrates the shape of the transition risk European governments will have to manage over the next two to three years.

We must start by examining the issue of procurement. The French Ministry of the Interior projected that deploying the new software and migrating existing data would take 18 to 24 months, while other reports estimated that a complete transition of the entire contract structure would take between 2027 and 2029. Interior Minister Laurent Nuñez stated that to bridge this gap, a transition period would be established to operate Palantir and Hapsvision side by side until 2027. The same issue recurs in Germany.

Germany's Federal Office for the Protection of the Constitution (BfV) confirmed in May 2026 that it would procure ArgonOS instead of Palantir, but for this procurement to actually become operational, a legislative amendment of over 700 pages redefining the authorities of the Federal Intelligence Service (BND) and the BfV must pass first. Germany's Federal Constitutional Court set the deadline for this legislative amendment for the end of 2026. The act of confirming procurement and the point at which that procurement becomes operational are tied to separate procedures.

The terms of a contract themselves can determine the speed of transition. In March 2025, the Ministry of the Interior of Baden-Württemberg signed a contract to adopt Palantir's Gotham software for €25 million over five years without an early termination clause. Although 92 percent of the Greens within the state coalition government voted in favor of immediately terminating the contract, a contract lacking an exit clause could not be overturned by political opposition alone. This contract demonstrates in numerical terms that failing to include termination conditions in advance of procurement contracts causes a state to forfeit its own bargaining power.

Issues surrounding personnel and data migration unfold outside contract documents. Agents at France's General Directorate for Internal Security (DGSI) are already

accustomed to Palantir's screen layout and interface mechanics, and the very method of storing information is structured to match the specifications of the U.S. system. Transitioning to a new program requires sequentially following steps to adapt existing workflows to new screens, retrain personnel, establish new data transmission paths, ensure ongoing investigations are not disrupted, and verify whether the system can handle actual workloads. The German Bundeswehr is undergoing a similar process.

Vice Admiral Thomas Daum of the Cyber and Information Domain Service announced in April 2026 that Palantir had been dropped as a candidate for the military cloud project pCloudBw, after which three entities—the German company Almato, the Berlin startup Oakrist Technologies, and the French company Hapsvision—underwent tests integrating live operational data during the summer of 2026. The final winning bidder is scheduled to be announced at the end of 2026. Dropping Palantir and deciding who will be newly selected remain separate issues for now.

The Netherlands carries another form of risk: procurement fragmentation. State Secretary for Defence Derk Boswijk announced in the House of Representatives on June 2, 2026, that Palantir would be replaced with a European alternative as quickly as possible, stating a target of two years to find a fully equivalent alternative. However, the government's subsequent response to the House contained only expressions like reviewing alternatives and reducing dependence, rather than a concrete deadline for termination. Behind this response lies the fact that contracts signed with Palantir within the Ministry of Defence were executed independently across departments, leaving no unified, government-wide registry of contracts.

State Secretary Boswijk himself admitted that cutting ties immediately could create a security vacuum in operational combat systems, defense logistics, and intelligence processing. The Dutch government itself has effectively testified to the fact that the pace of declaration differs from the pace of execution.

In the realm of allied operations, the direction of transition moves in reverse. NATO announced in 2025 that it had procured Palantir's Maven Smart System for use at Allied Command Operations. Whether this procurement announcement translates to actual operational scope as of 2026 remains a separate issue to be distinguished. However, as noted in Chapter 3 of this book, it is clear that the push to remove Palantir from domestic law enforcement and intelligence sectors is happening simultaneously alongside the trend of maintaining Palantir's position within military alliances.

Article 2 and Recital 24 of the European Union Artificial Intelligence Act exclude artificial intelligence systems for military, defense, and national security purposes from the scope of its application. This means that the withdrawal of domestic intelligence

agencies does not automatically carry over to procurement at the defense and NATO levels. This is precisely why the Netherlands Ministry of Defence cited interoperability requirements—the need to use the same system to exchange intelligence with NATO allies—as an obstacle to transition. On top of this, the U.S. CLOUD Act opens a pathway for U.S. investigative authorities to access information handled by U.S. entities regardless of server location. In intervals where the transition is incomplete, the reach of this law remains as well.

The maturity of alternative suppliers also determines the width of this transition period. Although Hapsvision recorded €200 million in revenue in 2025 after completing over twenty-five acquisitions since its founding in 2019, it remains a growing company compared to the long-established Palantir. Germany's final candidates, Almato and Oakrist Technologies, will also not see decisions on operational deployment until late 2026. Through the Cloud and AI Development Act, the European Commission set a goal to more than triple European data center capacity within five to seven years to meet corporate and public administration demand by 2035.

As of August 2026, this law is a regulation proposal submitted by the Commission and has not yet been enacted. The completion timeline for the plan to expand supply capacity itself already looks toward the mid-2030s.

The Anthropic incident of June 2026 forms the backdrop of all these transitions. On June 12, the U.S. government issued an export control directive to Anthropic ordering it to block access to Fable 5 and Mythos 5 for foreign nationals. Access was subsequently restored after export controls were lifted. This incident was not a permanent shutdown, but a tangible demonstration of the possibility that supply could be cut off at any time. While France, Germany, and the Netherlands seek alternatives at their own respective speeds, this possibility remains present.

What emerges consistently across the cases examined in this book is the fact that without exception, there is a gap of several years between the date of declaration and the date when the actual transition is completed. While bridging that gap, nations cannot avoid dual operation—using American technology and European alternatives side by side.

References and Sources

1. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, https://www.businesswire.com/news/home/20251215083215/en

2. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-

with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

3. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/

4. Unknown Author, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

5. Unknown Author, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

6. Unknown Author, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/

7. Eglė Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

8. Unknown Author, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-verkenningen

9. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', NCIA, 2025, https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system

10. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

11. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

12. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

13. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

14. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, https://www.anthropic.com/news/redeploying-fable-5

Conclusion 2: The Path of Resilient Openness

Between 2020 and 2024, across five agencies and four years, Switzerland's Federal Office of Public Health, Federal Statistical Office, Federal Office of Information Technology and Telecommunications, Federal Office for Defence Procurement (Armasuisse), and Money Laundering Reporting Office Switzerland repeatedly decided against adopting Palantir. Switzerland is not a country that tears out already-implemented programs like France or Germany. Instead, it is a country where an accumulation of agencies blocking entry from the very beginning has brought things to a point where there is little need for new persuasion.

In February 2026, the security media outlet Gendata reported that Switzerland rejected Palantir not because of inadequate performance, but because its proprietary and opaque internal structure, foreign judicial jurisdiction, and remote update mechanism were evaluated as uncontrollable sovereign risks. The Swiss assessment was that keeping data within Switzerland and adding protective clauses to contracts would not be enough to sufficiently prevent this risk. That is not to say, however, that Switzerland shut the door on foreign technology as a whole.

What Switzerland actually filtered out was a specific provider—Palantir—and its criteria were not nationality, but data location, jurisdiction, and control over updates.

Spain's actions show a choice of a similar nature. On July 1, 2026, the Spanish Prime Minister's Office issued guidelines instructing public enterprises under the state holding company—including telecommunications company Telefónica, defense company Indra, and shipbuilding company Navantia—not to enter into new contracts with Palantir. It did not invalidate existing contracts. The contract worth approximately 16.5 million euros between the Spanish Armed Forces Intelligence Center and Palantir remains in effect through November 2026. The Spanish government recognized from the policy design stage that preventing new contracts and terminating existing ones are separate issues. On the opposite end lies the case of Baden-Württemberg.

Locked in for five years and 25 million euros without an exit clause, this contract could not be overturned even with a 92 percent vote against it within the state coalition government. In February 2023, Germany's Federal Constitutional Court also ruled unconstitutional the legal bases under which the states of Hesse and Hamburg used Palantir-based systems for predictive policing, holding that analyzing citizens' telecommunications records and personal data broadly without legal authority infringes on the right to informational self-determination. When a contract lacks an exit

clause, it takes time for both political will and judicial rulings to translate into execution.

Placing these cases side by side reveals that the two extremes—complete closure and unconditional dependency—collapse in different ways. The limits of closure are confirmed by the admission of Dutch State Secretary for Defence Derk Boswijk. While stating that cutting ties with Palantir immediately could create security gaps in operational combat systems, defense logistics, and intelligence processing, he also acknowledged that there is currently no European alternative of comparable quality in military artificial intelligence. Closure unsupported by capability remains nothing more than a declaration.

Conversely, the limits of dependency are demonstrated by the Anthropic export control incident in June 2026 and the U.S. CLOUD Act, which grants U.S. law enforcement access regardless of server location. The text of treaties or contracts alone cannot prevent this exposure. The fact that the European Union Artificial Intelligence Act exempted AI systems meant for military, defense, and national security purposes from its scope is evidence that the European Union has already chosen to set different standards by sector rather than applying the same rules across all domains.

The Cloud and AI Development Act proposal put forward by the European Commission shows the path Europe has actually chosen between these two extremes. As of August 2026, this act is a regulatory proposal by the Commission rather than enacted legislation, and it includes as part of the AI Continent action plan the goal of more than tripling data center capacity over five to seven years to meet corporate and public administration demand by 2035. The four-tier sovereign assurance level design and sovereign termination clause examined in Chapter 4 of this book represent a method of isolating only the most sensitive domains while continuing to procure foreign technology in other areas, securing in advance the right to exit contracts.

This can be seen as an attempt to institutionalize safeguards in advance against the problem of exitless contracts experienced by Baden-Württemberg. The Eurostack vision by Francesca Bria and others, discussed in Chapter 5 of this book, stems from a similar awareness. The report states that restructuring digital infrastructure across Europe will require significant, multi-year investments. The exact total remains to be rechecked against the detailed line items of the original report.

This approach of pursuing openness and self-reliance simultaneously is not yet a finished result, but an ongoing attempt. How effective that attempt proves to be in practice hinges on several specific upcoming milestones. The German Bundeswehr will select the final provider for the pCloudBw project by the end of 2026. The German

Bundestag must pass legislation redefining intelligence agency authority by the end of 2026, in accordance with the deadline set by the Federal Constitutional Court. France's Ministry of the Interior has committed to co-operating Palantir and Hapsvision until 2027. The Palantir contract with the Spanish Armed Forces Intelligence Center ends in November 2026.

Whether these deadlines are actually met and whether the European alternatives filling those roles prove in operational practice a level of stability comparable to Palantir will be the next benchmarks for gauging whether this compromise—neither closure nor unconditional dependency—can hold.

Sources and References

1. Author Unknown, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/

2. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

3. Author Unknown, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

4. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

5. Eglė Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

6. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

7. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

8. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

9. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

10. European Commission, 'Cloud computing', Digital Strategy, 2026, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

11. Francesca Bria et al., 'EuroStack: A European Alternative for Digital Sovereignty', 2025, https://www.euro-stackreport.info/docs/EuroStack_2025.pdf

12. Author Unknown, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

13. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

14. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

Kim Kyung-jin
kimkj.com