

W H I T E P A P E R

The US–EU Cloud Data Conflict

GDPR, the CLOUD Act, and the Battle for Digital Sovereignty

A comparative analysis featuring Amazon Web Services and Schwarz Digits (STACKIT)

June 2026

Executive Summary

The digital economy rests on cloud infrastructure — but that infrastructure is governed by competing legal models. The European Union's GDPR treats personal data protection as a fundamental right. The United States relies on a sectoral approach, combining privacy laws with broad national-security and law-enforcement access powers such as the CLOUD Act and FISA. China follows a third model: data is subject to extensive state oversight through the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL). While PIPL is often compared to the GDPR because it contains consent, transparency, and transfer requirements, Chinese authorities retain broader statutory access powers than are generally accepted in the EU. As a result, multinational organisations increasingly evaluate cloud providers not only on technical capability, but also on the jurisdictional reach of the states to which those providers are exposed.

This conflict creates a genuine legal trap for multinational companies: they may simultaneously be required to hand over data (under US law) and forbidden from doing so (under EU law). There is currently no bilateral treaty that resolves this collision, leaving organisations to navigate the tension through a patchwork of contractual, technical, and architectural strategies.

This whitepaper examines the full legal landscape — including the CLOUD Act, GDPR Article 48, FISA Section 702, the EU Data Act, and the EU–US Data Privacy Framework — and illustrates the real-world consequences through a direct comparison of two cloud providers:

- Amazon Web Services (AWS), a US-headquartered hyperscaler that must manage GDPR compliance as a layer on top of its existing US legal obligations.
- Schwarz Digits / STACKIT, a fully EU-based cloud provider for which GDPR compliance is structural rather than contractual, and for which the CLOUD Act presents no jurisdictional basis.

The key finding is stark: the conflict is not one that any American cloud provider can fully resolve through contractual safeguards alone. The CLOUD Act's reach is jurisdictional — it follows the company, not the server. European sovereign cloud providers, by contrast, offer structural immunity that US hyperscalers cannot replicate without ceasing to be American entities. This distinction is increasingly shaping procurement decisions across regulated industries, public administration, and critical infrastructure.

1. The Core Legal Conflict

1.1 The Fundamental Tension

We live in a world where data crosses borders instantly — but the laws governing that data do not. The vast majority of global cloud infrastructure is operated by American companies: Amazon Web Services, Microsoft Azure, and Google Cloud collectively account for over 65% of the global cloud market. This means that even when data belongs to a European citizen, stored on a server in Frankfurt or Dublin, it remains under the control of a US-headquartered provider.

That single fact is the source of the conflict. A US company operating in the EU is simultaneously subject to two legal regimes that contradict each other on the question of government access to data.

The Legal Trap

A US cloud provider hosting EU data can be legally compelled by a US court to disclose that data to American authorities — and simultaneously legally forbidden by EU law from making that disclosure without consent. No contract can resolve this contradiction.

1.2 Why This Matters Now

The conflict has become more acute in recent years for several reasons. First, the CJEU's Schrems II ruling (2020) invalidated the EU–US Privacy Shield, explicitly citing US surveillance law as incompatible with EU fundamental-rights protections. [Footnote: Schrems II (Case C-311/18) is the 2020 Court of Justice of the European Union judgment that invalidated the EU–US Privacy Shield because EU citizens lacked protections and redress mechanisms considered essentially equivalent to those guaranteed under EU law.] [Footnote: The EU–US Privacy Shield was a transatlantic data-transfer framework that allowed certified US organisations to receive personal data from the EU until it was invalidated by Schrems II.] Second, FISA Section 702 was reauthorised in 2024. [Footnote: FISA Section 702 authorises US intelligence agencies to collect foreign-intelligence information from electronic communications service providers targeting non-US persons located outside the United States.] Since 2024, regulators have provided additional guidance through the first review of the EU–US Data Privacy Framework, while debates over the long-term durability of US surveillance reforms and the adequacy decision have continued into 2026.

2. The Relevant Legal Framework

2.1 US Legislation

The CLOUD Act (2018)

The Clarifying Lawful Overseas Use of Data Act grew out of the 1986 Electronic Communications Privacy Act and its Stored Communications Act — laws written for a pre-cloud era. The immediate trigger was the Microsoft Ireland case, in which a US appeals court ruled that the government could not force disclosure of emails stored on Microsoft's Dublin servers. Congress passed the CLOUD Act on March 23, 2018, explicitly to resolve this ambiguity — in the government's favour.

The CLOUD Act requires US-based providers to produce data stored anywhere in the world when served with a valid US legal process. It does not require the provider to notify the data subject. It does not require judicial review in the country where the data is stored. And it does not require the US government to go through Mutual Legal Assistance Treaty (MLAT) channels.

FISA Section 702

The Foreign Intelligence Surveillance Act's Section 702 authorises the collection of communications of non-US persons from US electronic communications service providers. Unlike the CLOUD Act (which is law-enforcement focused), FISA 702 is an intelligence tool. The procedural safeguards available to EU data subjects are limited compared with EU standards: collection is approved through programmatic oversight by the Foreign Intelligence Surveillance Court rather than individual warrants for each target, and non-US persons generally do not enjoy the same constitutional protections as US citizens. Schrems II identified FISA 702 as the primary obstacle because it directly concerns large-scale access to personal data transferred to US providers and because EU individuals historically lacked effective judicial redress. Secondary concerns include Executive Order–based surveillance authorities and the CLOUD Act itself. The CLOUD Act is not considered the primary Schrems II issue because it is targeted law-enforcement access, whereas FISA 702 enables broader intelligence collection. Schrems II did not prohibit transfers automatically; instead, it required exporters and providers to assess whether supplementary contractual, technical, and organisational measures can compensate for deficiencies in the destination country's legal regime.

2.2 EU Legislation

GDPR (2018) — General Data Protection Regulation

The cornerstone of EU data protection, GDPR treats privacy as a fundamental right under the EU Charter. Key provisions in this conflict include:

- Article 48: Court orders or judgements from third countries are only valid if based on an international agreement such as an MLAT. The CLOUD Act bypasses MLATs entirely.
- Chapter V (Articles 44–49): Transfers of personal data to third countries require either an adequacy decision, Standard Contractual Clauses (SCCs), or another approved mechanism.
- Article 83: Violations carry fines of up to €20 million or 4% of global annual turnover.

EU Data Act (2023/2854) — Effective September 2025

Chapter VII of the EU Data Act requires cloud providers operating in the EU to implement technical, legal, and organisational measures to prevent unlawful non-EU government access to non-personal data stored in the EU. Personal data remains primarily governed by the GDPR

rather than the Data Act. The distinction does not imply that personal data is less important; rather, the GDPR already contains a mature framework governing international transfers and foreign-government access. When a provider receives a CLOUD Act-type demand, it must assess whether the request is reasoned, specific, and proportionate and, where appropriate, challenge or resist access requests that conflict with EU law.

The EU–US Data Privacy Framework (DPF)

The DPF is the current mechanism for legitimising commercial data transfers between the EU and the US. However, it does not prevent US authorities from issuing CLOUD Act or FISA 702 demands to certified companies. Its predecessors — Safe Harbour (2000) and Privacy Shield (2016) — were both invalidated by the CJEU. The European Data Protection Board's November 2024 review called for re-evaluation within three years.

NIS2 Directive and DORA

NIS2 (applicable from October 2024) requires essential entities to assess ICT supply-chain security, including provider exposure to non-EU government access demands. DORA (January 2025) requires financial entities to assess ICT concentration risk. [Footnote: DORA – the Digital Operational Resilience Act – is the EU framework governing operational resilience, cyber risk, third-party ICT risk, and incident management in the financial sector.] The CLOUD Act can create a concentration risk because many critical European organisations rely on a small number of US hyperscalers that are subject to the same foreign-access laws, creating a common legal dependency that may affect multiple institutions simultaneously.

Law / Framework	Jurisdiction	Key Effect on the Conflict
CLOUD Act (2018)	United States	Compels US providers to disclose data stored anywhere globally
FISA Section 702	United States	Enables intelligence collection from US providers on non-US persons
GDPR Art. 48	European Union	Invalidates foreign court orders not based on international agreements
EU Data Act (2025)	European Union	Requires providers to actively resist unlawful non-EU access demands
EU–US DPF	EU–US bilateral	Legitimises commercial transfers but does not block government access
NIS2 / DORA	European Union	Requires risk assessment of provider exposure to foreign government access

3. Case Study — Amazon Web Services (AWS)

3.1 The Challenge: Compliance as a Layered Problem

Amazon Web Services is the world's largest cloud provider, with a 31% global market share. Its German and European operations are substantial: AWS operates dedicated EU regions in Frankfurt (eu-central-1), Ireland, Spain, Italy, Sweden, and France, and has committed €7.8 billion to build an 'AWS European Sovereign Cloud' in Brandenburg, Germany.

Yet AWS remains a US company. Headquartered in Seattle, incorporated under US law, and listed on a US stock exchange, it is — by definition — subject to the CLOUD Act. No amount of European infrastructure investment changes this foundational legal reality.

3.2 AWS's GDPR Strategy

AWS's approach to GDPR compliance is comprehensive and multilayered, built around four pillars:

Contractual Safeguards

AWS offers a GDPR-compliant Data Processing Addendum (DPA) that automatically applies to all EU customers. The DPA incorporates the European Commission's Standard Contractual Clauses (SCCs), which serve as a recognised legal transfer mechanism under GDPR Chapter V. In other words, the SCCs are themselves the transfer mechanism rather than merely a description of one. AWS has also issued a Supplementary Addendum committing to redirect governmental data requests to customers whenever legally and operationally possible, meaning AWS will seek to have the request served directly on the customer where permitted. AWS also commits to notify customers where lawful and to challenge requests that are overly broad or conflict with applicable law.

Technical Controls

AWS offers customers granular control over data location, encryption in transit and at rest, customer-managed encryption keys, and the Nitro System. Whether a US authority can obtain intelligible data depends heavily on key management. If AWS controls the key, AWS may be technically capable of providing decrypted data. If the customer exclusively controls and stores the key outside AWS's control, neither AWS nor a court can simply 'crack' modern encryption; instead, the authority would need lawful access to the key holder or another technical avenue.

Certifications

AWS holds ISO 27001, ISO 27017, ISO 27018, ISO 27701, and German BSI C5 attestations. These certifications do not certify immunity from the CLOUD Act. Rather, they assess security, governance, transparency, and operational controls. A provider can therefore be both CLOUD Act-exposed and C5-compliant. STACKIT does hold a C5 attestation rather than merely seeking one.

The European Sovereign Cloud Initiative

In its most ambitious response to the sovereignty challenge, AWS is establishing a new corporate entity — AWS European Sovereign Cloud — as an EU-law company with its own management structure, operated from Brandenburg, Germany. The intent is to create a legally distinct entity that is not operationally dependent on US parent company systems or personnel.

The Unresolvable Tension

AWS's contractual commitments to resist government requests are genuine — but they are promises, not barriers. A US federal court order supersedes any contractual commitment. AWS's Supplementary Addendum commits to 'actively challenge' overreaching requests, not to refuse them. The CLOUD Act's reach is jurisdictional and cannot be waived by contract.

3.3 Residual Risk Assessment

Despite AWS's extensive compliance infrastructure, EU customers face a residual legal risk that cannot be fully mitigated through contractual or technical means alone. The EU Data Act requires providers to implement measures and make genuine efforts to assess, challenge, and resist unlawful third-country access requests. However, the Act does not guarantee success. Compliance is generally assessed on the adequacy of the provider's measures and efforts rather than on an absolute obligation to defeat every foreign demand.

4. Case Study — Schwarz Digits / STACKIT

4.1 Origin and Positioning

STACKIT is the cloud platform of Schwarz Digits, the IT and digital division of Schwarz Group — parent company of Lidl and Kaufland, Europe's largest retailer by revenue (approximately €155 billion in FY2024). STACKIT began as internal infrastructure for Schwarz Group's own digital transformation, processing data across thousands of European retail locations. It was opened to external customers and public sector clients in 2021.

STACKIT is not an American company with European servers. It is a German company, incorporated under German law, headquartered in Neckarsulm, Baden-Württemberg, with no US parent company and no US stock market listing. This single fact is the foundation of its GDPR and sovereignty positioning.

4.2 STACKIT's GDPR Position

For STACKIT, GDPR compliance is structural rather than contractual. Because STACKIT is an EU entity with no US parent:

- The CLOUD Act has no jurisdictional basis to compel data disclosure — there is no US nexus.
- FISA Section 702 does not apply — STACKIT is not a US electronic communications service provider.
- All data is stored exclusively in EU data centres (currently Germany and Austria), meaning no cross-border transfer mechanisms such as SCCs are required for data in transit between STACKIT and its EU customers.
- Client-side encryption means STACKIT itself cannot access customer data — satisfying both GDPR Article 25 (data protection by design) and providing a technical barrier to any hypothetical future access demand.

4.3 Certifications and Standards

STACKIT holds the following certifications relevant to EU data protection:

- ISO 27001 (based on BSI IT-Grundschutz) for IaaS and PaaS services including Compute Engine, Network & Security, Block Storage, and Object Storage.
- C5 (Cloud Computing Compliance Criteria Catalogue) attestation from the German Federal Office for Information Security (BSI) — the highest German standard for cloud security.
- ISAE 3000 (SOC 2, Type 1) and ISAE 3402 (Type 1) for international compliance requirements.
- TISAX assessment for automotive industry data protection requirements.

4.4 The Sovereignty Marketing Strategy

STACKIT uses its EU-only jurisdiction as a central competitive differentiator, particularly in B2B sales to regulated industries. The messaging is explicit: organisations must choose between handing sensitive data to providers bound by the US CLOUD Act, or retaining genuine digital sovereignty. Key elements of this strategy include:

- Direct reference to CLOUD Act exposure in sales materials and partner communications.
- Targeting compliance officers and CTOs in financial services, healthcare, public administration, and critical infrastructure — sectors where US government access would be most damaging.
- Strategic partnerships with SAP (RISE with SAP on STACKIT, announced October 2024), SentinelOne, CrowdStrike, MicroStrategy, and others — positioning STACKIT as a sovereign-first ecosystem, not merely a sovereign data centre.

Strategic Positioning Quote

"European organizations are now at a crossroads: they can either hand their most sensitive data to foreign hyperscalers bound by the US CLOUD Act, or they can reclaim their digital independence on home soil." — STACKIT marketing positioning, 2025

Notably, this positioning is deployed with precision rather than mass-market noise. In keeping with Schwarz Group's corporate culture, there are no large-scale consumer advertising campaigns. The sovereignty argument is a B2B weapon — aimed at procurement boards, not billboards.

5. Head-to-Head Comparison

Dimension	AWS (Amazon DE)	STACKIT (Schwarz Digits)
Headquarters	Seattle, USA (EU operations: Ireland)	Neckarsulm, Germany
CLOUD Act exposure	Yes — inherent, cannot be waived	None — no US jurisdictional nexus
FISA 702 exposure	Yes — US provider of electronic comms	No — not a US provider
GDPR approach	Contractual (DPA, SCCs, Supplementary Addendum)	Structural (EU entity, no foreign nexus)
Data residency	Customer-controlled; EU regions available	Germany and Austria exclusively
Encryption model	AWS-managed or customer-managed keys	Client-side; provider cannot access data
Key certifications	ISO 27001/17/18/27701, C5, CISPE	ISO 27001 (BSI-IT Grundschutz), C5, ISAE 3000/3402, TISAX
Government request policy	Challenge overreaching requests; notify customers	No US authority basis; EU law exclusively
Sovereignty claim	Partial — operational sovereignty, not legal	Full — legal and operational sovereignty
Residual legal risk for EU customers	Exists — US court order can override contracts	Minimal — no cross-jurisdictional exposure
Market positioning	Global hyperscaler with EU sovereignty product	European-first sovereign cloud challenger

6. How Companies Navigate the Conflict

In the absence of a bilateral EU–US treaty resolving the CLOUD Act / GDPR tension, organisations have developed a range of mitigation strategies — each with different risk profiles.

6.1 Contractual Mechanisms

Data Processing Agreements (DPAs) and Standard Contractual Clauses (SCCs) are the standard tools for legitimising EU–US data transfers. However, following Schrems II, the EDPB confirmed that contractual measures alone cannot address exposure to foreign surveillance laws. [Footnote: EDPB stands for the European Data Protection Board, the body that coordinates GDPR interpretation and enforcement across EU and EEA data-protection authorities.] SCCs provide a transfer mechanism; they do not provide immunity from a CLOUD Act order.

6.2 Technical Architecture: Encryption as a Shield

Customer-controlled encryption with keys held outside US infrastructure can render a provider technically incapable of decrypting customer data. AWS's KMS and CloudHSM services support this model, but the precise level of protection depends on who ultimately controls the keys. STACKIT's client-side encryption model is designed so that the provider itself has no decryption capability. Accordingly, if the provider does not possess the key, neither a US authority nor any other authority can obtain decrypted data directly from the provider.

6.3 Sovereign Cloud Products

Microsoft, AWS, and Google have all launched products marketed as providing EU data sovereignty. The marketing claims are generally qualified by contractual terms and service documentation. While these offerings provide stronger data residency, operational control, and access-management guarantees, they do not universally claim immunity from all foreign laws. Legal analyses continue to distinguish operational sovereignty from complete jurisdictional sovereignty.

6.4 Switching to EU-Native Providers

The most structurally clean solution is to move workloads to providers with no US nexus: STACKIT, OVHcloud (France), IONOS (Germany), or Hetzner (Germany). The EU Data Act (September 2025) now legally requires cloud providers to support switching — reducing the lock-in barrier that historically kept organisations tied to hyperscalers. European sovereign cloud spending is projected to grow 83% in 2026.

6.5 Transfer Impact Assessments (TIAs)

Before any cross-border transfer, organisations must conduct a Transfer Impact Assessment following the EDPB's six-step framework: (1) map transfers; (2) identify the transfer mechanism; (3) assess destination country laws; (4) implement supplementary safeguards; (5) document steps; (6) reassess periodically. TIAs are now a legal requirement, not optional due diligence.

6.6 MLAT Channels

When US law enforcement issues a CLOUD Act request directly to a European business, the correct response is to redirect to the Mutual Legal Assistance Treaty process — which includes

stronger procedural safeguards. However, MLAT requests can take years; the CLOUD Act was designed in part to circumvent this delay.

7. Strategic Outlook

7.1 The EU Response: Building Structural Immunity

The EU's response to the CLOUD Act has evolved from contractual workarounds to structural alternatives. [Footnote: The Data Act is Regulation (EU) 2023/2854, which among other objectives addresses cloud switching and certain third-country government access requests.] [Footnote: Gaia-X is a European initiative that promotes interoperable, transparent, and sovereign digital infrastructure standards.] [Footnote: EUCS is the proposed European Cybersecurity Certification Scheme for Cloud Services developed under the EU Cybersecurity Act.] [Footnote: CAIDA refers to the proposed Cloud and AI Development Act, intended to strengthen European cloud and AI capacity and digital sovereignty.]

7.2 The US Response: Jurisdictional Subsidiaries

The US hyperscalers' response — creating legally distinct EU subsidiaries such as AWS European Sovereign Cloud — is the most ambitious attempt to bridge the conflict. Whether these structures genuinely insulate EU data from US government demands will ultimately be decided by a court. Until that test arrives, legal uncertainty remains.

7.3 The Geopolitical Dimension

The CLOUD Act conflict is no longer purely a legal or technical issue. It has become a question of digital geopolitics. The European Commission's repeated emphasis on 'digital sovereignty' reflects a strategic judgement that dependency on non-EU cloud infrastructure creates a structural vulnerability — not merely a compliance risk. This has accelerated public sector investment in EU-native cloud infrastructure across Germany, France, and the Nordic countries.

The Bottom Line

There is currently no bilateral EU-US agreement specifically resolving the CLOUD Act / GDPR conflict. A direct CLOUD Act demand to a US provider automatically constitutes a potential GDPR violation. Until a comprehensive international treaty bridges the two systems, organisations handling sensitive EU personal data face a binary choice: accept residual legal risk with US hyperscalers, or achieve structural immunity through EU-native providers.

8. Key Terms and Abbreviations

Term	Definition	Relevant Section
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (US, 2018) — authorises US government access to data held by US providers globally	Sections 1, 2
GDPR	General Data Protection Regulation (EU, 2018) — the primary EU personal data protection framework	Sections 1, 2
FISA 702	Foreign Intelligence Surveillance Act Section 702 — authorises US intelligence collection from US providers on non-US persons	Section 2
SCC	Standard Contractual Clauses — EU-approved contractual mechanisms for cross-border data transfers	Sections 2, 6
DPA	Data Processing Agreement — contract between data controller and processor under GDPR Article 28	Section 6
MLAT	Mutual Legal Assistance Treaty — international framework for cross-border law enforcement cooperation	Sections 2, 6
TIA	Transfer Impact Assessment — mandatory assessment before transferring personal data outside the EEA	Section 6
C5	Cloud Computing Compliance Criteria Catalogue — BSI (German Federal Office for Information Security) cloud security standard	Sections 3, 4
DPF	EU-US Data Privacy Framework — current mechanism legitimising commercial EU-US data transfers	Section 2
BYOK	Bring Your Own Key — encryption key management model where the customer, not	Section 6

	the provider, controls decryption keys	
NIS2	Network and Information Security Directive 2 — EU cybersecurity framework applicable from October 2024	Section 2
DORA	Digital Operational Resilience Act — EU financial sector ICT resilience framework applicable from January 2025	Section 2

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute legal advice. The legal landscape surrounding GDPR, the CLOUD Act, and related frameworks is subject to ongoing judicial and legislative development. Organisations should seek qualified legal counsel before making compliance decisions. All company information is based on publicly available sources as of May 2025.

SECOND-PASS LEGAL REVIEW NOTES (JUNE 2026)

Schrems II focused primarily on FISA 702, Executive Order 12333 concerns, and inadequate redress mechanisms. The CLOUD Act remains important but was not the principal basis of the judgment. The EDPB's first review of the EU-US Data Privacy Framework in November 2024 generally welcomed implementation while continuing scrutiny. The EU Data Act's third-country access provisions apply specifically to non-personal data; personal data remains primarily governed by the GDPR. C5 certification evaluates security and governance controls and does not certify immunity from the CLOUD Act. AWS European Sovereign Cloud materially improves operational sovereignty, but its ability to withstand a future jurisdictional challenge remains legally untested. Other European cloud providers of meaningful scale include OVHcloud, IONOS, Scaleway, Open Telekom Cloud, Cleura, and Exoscale.