

IMPOSSIBLE CLOUD

WHITE PAPER · SEPTEMBER 2026

The US CLOUD Act and European data sovereignty

What the Act can and cannot do, how it meets NIS2
and UK law, and what technology leaders should ask.

A BRIEFING FOR

**Chief technology officers, IT directors
and their boards**

Covers: US CLOUD Act (2018) · FISA Section 702 · GDPR Article 48
EU Data Act · NIS2 Directive · UK Cyber Security and Resilience Bill

Impossible Cloud GmbH, Hamburg, Germany. Position as at 24 September 2026. Not legal advice.

The US CLOUD Act and European data sovereignty

01 EXECUTIVE SUMMARY

Control, not location, decides access

Under the US CLOUD Act, the legal identity of your provider, not the location of your data, decides who can compel access to it. For European organisations that turns cloud procurement into a question of jurisdiction, and one that regulators now expect boards to answer on the record.

1. **Jurisdiction follows control.** A provider subject to US jurisdiction must produce data in its possession, custody or control, wherever that data is stored.
2. **A European data centre is not a legal barrier.** The conflict with GDPR Article 48 is real, and no EU-level agreement with the United States exists to resolve it.
3. **The CLOUD Act is one route among several.** US intelligence access runs separately under FISA Section 702, and providers can be barred from telling you a demand exists.
4. **NIS2 and the UK's Cyber Security and Resilience Bill are security regimes, not sovereignty laws.** Both, however, make supplier risk, including jurisdictional risk, an auditable board responsibility.
5. **Sovereignty reduces exposure; it does not eliminate lawful access.** It replaces foreign compelled access with access under your own legal order and its safeguards, and it should be decided workload by workload.

02 THE LAW

What the CLOUD Act is

The Clarifying Lawful Overseas Use of Data Act became law on 23 March 2018, inside the US federal spending bill. It settled *United States v Microsoft*, in which Microsoft had refused a warrant for email held in Ireland, and the Supreme Court then declared that case moot.

The Act has two parts.

- **Compelled disclosure (18 U.S.C. § 2713).** Providers of electronic communication

or remote computing services must preserve and disclose content and records within their possession, custody or control, whether the data sits inside or outside the United States.

- **Executive agreements (18 U.S.C. § 2523).** The United States may agree with a "qualifying foreign government" that each side's authorities can serve orders directly on the other's providers. The UK agreement has been in force since October 2022 and the Australian agreement since January 2024.

The decisive point for European buyers is scope. The US Department of Justice has stated that the Act extends US jurisdiction to no new foreign company; whether a provider is caught depends on ordinary US rules on contacts with the United States. A US parent, a US subsidiary or a material US business can each supply that connection. Where it exists, the Act applies regardless of where the servers stand.

03 SCOPE

What it can and cannot do

The Act is narrower than its reputation in some respects and wider in others. The table sets out the position as the statute and the Department of Justice describe it.

Question	Position
Can it reach data stored in Europe?	Yes, if the provider is subject to US jurisdiction and the data is within its control. Location is irrelevant.
Does it apply to a provider with no US connection?	No. The Act creates no new jurisdiction. The line is drawn by US due process case law, not by a fixed test.
Must the customer be told?	No. Courts can order a provider to keep a demand secret under 18 U.S.C. § 2705(b).
Can the provider challenge a demand?	Yes, within 14 days. The statutory comity route applies only where the target is not a US person and disclosure would breach the law of a qualifying foreign government. No EU member state currently qualifies, so European customers rely on weaker common law comity.
Can it compel decryption?	No new power. The Justice Department calls the Act "encryption neutral". Where only the customer holds the keys, the provider can produce only ciphertext.
Does it cover intelligence collection?	No. National security access runs under FISA, a separate regime (section 04).
Does it require data to be kept in the United States?	No. It is indifferent to storage location in both directions.

Table 1. Powers and limits of the CLOUD Act. Sources: 18 U.S.C. §§ 2703, 2713; US Department of Justice white paper,

INTENT AND EFFECT

The Act was designed to speed up access to evidence in serious crime, replacing slow mutual legal assistance requests between governments. Its effect, for any organisation using a US-controlled provider, is that a foreign court can compel access without the involvement of the customer's own authorities. It should be read as a lawful, due process instrument. It should not be read as a guarantee that European law will be weighed before disclosure, because for EU customers no statutory mechanism requires that.

04 BEYOND THE CLOUD ACT

The wider US access landscape

The CLOUD Act governs criminal evidence. It is not the only exposure a European customer of a US-controlled provider carries, and arguably not the largest.

- **FISA Section 702.** It authorises surveillance of non-US persons located outside the United States, with the compelled assistance of US communications providers, without an individual warrant. The statute lapsed on 12 June 2026 after Congress failed to agree a reauthorisation. Certifications approved before the lapse remain in force until March 2027, so collection continues while negotiations do.
- **Secrecy.** FISA orders carry permanent non-disclosure obligations, and criminal demands can carry court-ordered gag provisions. The customer may never learn that access occurred.
- **Service availability.** A separate risk from access is withdrawal of service. In 2025 the Chief Prosecutor of the International Criminal Court lost access to his Microsoft email after US sanctions were imposed. Microsoft has said it did not suspend services to the Court itself. The case is cited in UK parliamentary research as evidence that dependency risk is not theoretical.

These are distinct legal mechanisms, and they should be assessed separately. A provider's answer on the CLOUD Act says nothing about its exposure to FISA or to sanctions.

05 EUROPE

Ramifications for European organisations

The provider receives the demand, but the regulatory consequence lands on the

customer as data controller. GDPR accountability does not transfer to a supplier.

- **GDPR Article 48.** A third-country court order to transfer personal data is recognised only where it rests on an international agreement, such as a mutual legal assistance treaty. In their 2019 joint assessment the EDPB and EDPS concluded that, without such an agreement, a CLOUD Act disclosure has no lawful basis under GDPR. The EDPB's guidelines on Article 48, finalised in June 2025, confirm that such an order does not in itself make a transfer lawful.
- **No resolving agreement.** EU and US negotiators have discussed an e-evidence agreement since 2019. None has been concluded, so the conflict has no bilateral mechanism for resolution.
- **The Data Privacy Framework is not the answer to this question.** The Framework gives a legal basis for transfers organisations choose to make. It does not stop a provider being compelled. It was upheld by the EU General Court on 3 September 2025 (*Latombe*, T-553/23), and an appeal to the Court of Justice is pending (C-703/25 P). Its two predecessors were struck down.
- **Non-personal data is now in scope too.** The EU Data Act, applicable since 12 September 2025, requires cloud providers to take measures against third-country government access to non-personal data held in the EU where that access conflicts with EU or national law (Article 32). They must also publish the jurisdiction their infrastructure is subject to (Article 28). Industrial data, designs and trade secrets therefore now sit inside the same analysis.
- **"Sovereign" offerings from US providers.** On 10 June 2025, Microsoft France's director of public and legal affairs told a French Senate inquiry, under oath, that he could not guarantee French citizens' data would never be passed to US authorities without French consent. The answer was candid and legally accurate: European data centres and contractual commitments do not change the parent company's legal obligations.

SOVEREIGNTY IS NOT ZERO ACCESS

The EU e-Evidence Regulation has applied since 18 August 2026. Judicial authorities in one member state can now order a provider in another to produce data within 10 days, or 8 hours in an emergency. A European provider is therefore subject to lawful access, but under EU law, EU courts and the Charter of Fundamental Rights. That is the substance of the sovereignty argument, and it should be stated that way to boards and auditors.

Policy is moving in the same direction. On 3 June 2026 the European Commission

proposed a Cloud and AI Development Act, which includes a single EU-wide framework for assessing cloud and AI sovereignty. It remains a proposal.

06 NIS2

Where sovereignty fits in NIS2

NIS2 does not require European providers or data localisation. It requires you to assess, justify and evidence your supplier choices, and jurisdiction is a legitimate part of that assessment.

The NIS2 Directive (EU) 2022/2555 was due for national transposition by 17 October 2024. Transposition has been uneven; Germany's implementing law, for example, entered into force on 6 December 2025. The provisions that bear on this question are consistent across member states.

Provision	Requirement	Relevance to jurisdiction
Article 20	Management bodies approve and oversee cybersecurity risk measures and can be held liable	Supplier jurisdiction becomes a board decision, not a procurement detail
Article 21(2)(d) and 21(3)	Supply chain security, taking account of each direct supplier's vulnerabilities and security practices	A compelled access route, or a sanctions-driven withdrawal of service, is a supplier risk to be assessed
Article 21(2)(c)	Business continuity, backup management and crisis management	Continuity plans should test whether backups remain available if a supplier's home government intervenes
Article 22	EU coordinated risk assessments of critical supply chains, covering technical and non-technical factors	Non-technical factors include undue influence by a third country over suppliers
Article 23	Early warning within 24 hours, notification within 72 hours, final report within one month	Incident duties remain yours whoever hosts the data
Article 34	Fines up to EUR 10 million or 2% of worldwide turnover (essential entities); EUR 7 million or 1.4% (important entities)	The cost of an undocumented supplier decision is explicit

Table 2. NIS2 provisions relevant to supplier jurisdiction. Source: Directive (EU) 2022/2555.

Where it is heading. On 20 January 2026 the Commission proposed a revised Cybersecurity Act (CSA2) with targeted NIS2 amendments. It would create the EU's first

horizontal ICT supply chain framework: the Commission could designate high-risk suppliers and require NIS2 entities to phase out their components from key ICT assets, with fines of up to 7% of worldwide turnover. Political agreement is targeted for early 2027. The framework is not directed at any named country, but it confirms that the EU now treats supplier jurisdiction and foreign interference as security matters.

07 UNITED KINGDOM

The UK position

The UK has no dedicated data sovereignty statute before Parliament. The live instrument is the Cyber Security and Resilience (Network and Information Systems) Bill, the UK's counterpart to NIS2, and sovereignty is being argued around it rather than written into it.

Cyber Security and Resilience Bill. Introduced on 12 November 2025, it completed its Commons stages on 16 June 2026 and has been in Lords committee since 1 September 2026, with report stage provisionally set for 26 October 2026. It amends the NIS Regulations 2018. As introduced, it:

- brings medium and large managed service providers, data centres of 1 MW and above, and designated critical suppliers into regulation;
- introduces an initial incident notification within 24 hours and a full report within 72 hours, copied to the National Cyber Security Centre;
- introduces turnover-linked penalties; and
- leaves most detailed obligations, including supply chain duties, to secondary legislation, so full effect is not expected before around 2028.

Sovereignty. Amendments seeking a review of cyber risks from foreign ownership and interference were tabled in the Commons, and calls for a statutory digital sovereignty strategy continue in the Lords. House of Lords Library research published in July 2026 records that the UK has not pursued an explicit digital sovereignty strategy. In March 2026 a DSIT minister confirmed that no central assessment had been made of the CLOUD Act's implications for UK government data.

Data protection. The Data (Use and Access) Act 2025 received Royal Assent on 19 June 2025. It replaces the test for international transfers with a requirement that protection in the destination is not materially lower than in the UK. Transfers to certified US organisations can rely on the UK Extension to the EU-US Data Privacy Framework.

A UK NUANCE

Because of the UK-US Data Access Agreement, the UK is a qualifying foreign

government under the CLOUD Act. A US provider can therefore invoke the statutory comity challenge for UK customers, a route not available to EU customers. It is a procedural protection, not a bar to access.

08 COMPARISON

The regimes side by side

Only one of these instruments creates foreign access; the others govern how you must manage the risk it creates.

	US CLOUD Act	EU NIS2	UK Cyber Security and Resilience Bill	EU Data Act
Nature	Law enforcement access power	Cybersecurity obligations	Cybersecurity obligations	Data access, portability and cloud switching rules
Status (September 2026)	In force since March 2018	In force; national transposition uneven	In the House of Lords; Royal Assent expected late 2026 or 2027	Applicable since September 2025
Who it binds	Providers subject to US jurisdiction	Essential and important entities in listed sectors	Operators of essential services, digital and managed service providers, data centres, designated critical suppliers	Data holders and cloud providers serving the EU
Stance on jurisdiction	Location irrelevant; control decides	Supplier risk must be assessed; no localisation mandate	Supply chain duties to follow in secondary legislation; no sovereignty duty	Providers must resist unlawful third-country access and publish their jurisdiction
What it asks of you	Nothing directly; it acts on your provider	Board-approved risk measures, supplier assessment, 24/72-hour reporting	Resilience measures and 24/72-hour reporting, once in force	Use switching and transparency rights when choosing providers

Table 3. How the four regimes relate. Position as at 24 September 2026.

09 DECISION FRAMEWORK

What technology leaders should do

Treat sovereignty as a classification decision, not a blanket policy. Most estates contain workloads where US-controlled services are an acceptable, documented risk, and others

where they are not.

Step 1: classify. Identify the data where compelled foreign access would be unacceptable: regulated personal data, public sector and health records, legally privileged material, trade secrets, and the backups that protect all of them. Backups are routinely overlooked, yet they hold a complete copy of everything else.

Step 2: put eight questions to every provider, including the one you are currently using. Ask for written answers.

1. Which legal entity contracts with us, and who ultimately controls it?
2. Does any company in the group have a US parent, subsidiary, office or material US business?
3. Can any non-EU entity or employee reach production systems, identity and access management, encryption keys, support tooling, logs or metadata?
4. Who holds the encryption keys, and can you produce plaintext if ordered?
5. Where is your jurisdiction statement under Data Act Article 28 published, and which clause of our contract references it?
6. What measures have you taken under Data Act Article 32, and will you challenge and notify us of any third-country demand where the law allows?
7. Which sub-processors, hardware suppliers and facility operators are involved, and under which jurisdictions?
8. What does it cost, in time and money, to leave? The Data Act removes switching charges from 12 January 2027.

Step 3: record the decision. Minute the classification, the answers and the residual risk at the level NIS2 Article 20 requires. An auditor will ask not whether you chose a US or European provider, but whether you understood the choice.

10 IMPOSSIBLE CLOUD

Where Impossible Cloud fits

Impossible Cloud addresses the storage layer of this problem: object storage for data and backups, operated by a European company under European law. It is one component of a sovereign architecture, not a substitute for one.

Impossible Cloud GmbH is headquartered in Hamburg, Germany, and was founded in 2021. It provides S3-compatible object storage, sold through distributors and partners, in customer-selected regions including Germany, the Netherlands, Poland, Denmark

and the United Kingdom. Regions are geo-fenced: data stays in the region chosen at bucket level.

Requirement	What Impossible Cloud provides	What remains with the customer
Jurisdiction (NIS2 Art. 21(3); Data Act Art. 28)	German company under EU and German law; identity and access management operated in Germany	Confirming the legal position with counsel for your own risk register
Backup and continuity (NIS2 Art. 21(2)(c))	Object Lock immutability and versioning; no egress fees on restore	Backup policy, retention periods and restore testing
Access control (NIS2 Art. 21(2)(i) and (j))	Role-based access control and multi-factor authentication	User governance and privileged access reviews
Encryption (NIS2 Art. 21(2)(h))	Encryption in transit and at rest, including server-side encryption	Client-side encryption and key custody for the most sensitive data
Assurance	ISO/IEC 27001 certified company; data centres certified to ISO 27001, SOC 2 and PCI DSS	Supplier due diligence and periodic review
Portability (Data Act switching rules)	Full S3 API compatibility; no egress or API charges	Exit planning

Table 4. Shared responsibility at the storage layer.

THE LIMITS, STATED PLAINLY

No provider can promise that data will never be subject to lawful access. Data held in Impossible Cloud's EU regions is subject to EU and member state law, including the e-Evidence Regulation. Buyers should apply the eight questions above to Impossible Cloud as rigorously as to any other supplier and obtain the answers in writing.

11 CONCLUSION

Know which legal order can reach your data

The CLOUD Act has not changed since 2018; European regulation around it has. GDPR, the Data Act and NIS2 now require organisations to know which legal order can reach their data, to justify that exposure and to evidence the decision at board level. The UK is converging on the same expectations through the Cyber Security and Resilience Bill, without yet framing them as sovereignty.

The practical response is neither to abandon US platforms nor to treat European hosting as a guarantee. It is to classify data, question every supplier on control rather than location, and place the workloads that matter most, backups first, with providers whose legal accountability matches your own.

REFERENCES

Sources

- CLOUD Act, Division V of H.R. 1625 (US Department of Justice): [justice.gov](https://www.justice.gov)
- 18 U.S.C. § 2703, including subsection (h) (Cornell Legal Information Institute)
- Cross-Border Data Sharing Under the CLOUD Act, R45173 (Congressional Research Service)
- Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (US Department of Justice, April 2019)
- Section 702 of FISA: 2026 Resource Page (Brennan Center for Justice)
- FISA 702, a key US spy tool, has lapsed (NPR, 12 June 2026)
- The EU-US Data Privacy Framework Upheld at First Instance: *Latombe v Commission* (European Data Protection Law Review, 2026)
- Digital and technology policy and national sovereignty (House of Lords Library, July 2026)
- Cybersecurity Package: Questions and Answers (European Commission, January 2026)
- Cyber Security and Resilience (Network and Information Systems) Bill: stages (UK Parliament)
- Cyber Security and Resilience Bill 2024-26, CBP-10442 (House of Commons Library)
- Regulation (EU) 2023/1543 on electronic evidence; Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2023/2854 (Data Act)
- Impossible Cloud: compliance, data residency and company information (impossiblecloud.com)

This paper is a technical and policy briefing, not legal advice. Organisations should take legal advice on their own position. Position as at 24 September 2026. © 2026 Impossible Cloud GmbH.