01 The duty
02 The data
03 The dependency
04 The evidence
05 The upside

Where your data lives, and who can compel it

Residency answers where data sits. It does not answer who can reach it. The board's question is jurisdiction: which laws bind the entity holding the keys, and what happens when two of them conflict.

THE COMMISSION'S MEASURE

48

CRITERIA

Eight weighted categories, scored SEAL-0 to SEAL-4 in the Cloud Sovereignty Framework.

SEAL-2

FLOOR

The minimum required of bidders for the Commission's own sovereign cloud framework, awarded April 2026.

REACH

18 Aug 2026

E-EVIDENCE

European Production Orders now bind any provider serving the Union, wherever established.

3 Oct 2027

EXPIRY

The UK and US data access agreement lapses unless both governments renew it.

Suppliers sell three properties as one word

The European Commission's Cloud Sovereignty Framework separates what suppliers merge. Data sovereignty is defined as the protection, control and independence of data assets and AI services within the Union, with confinement of storage and processing to European jurisdictions as one contributing factor among several. Operational sovereignty is defined separately, as the practical ability of European actors to run, support and evolve a technology independently of foreign control.[1] Residency appears as an input to the first, never as a property of its own, which is why a supplier who answers with the location of a data centre has answered a different question from the one asked.

The framework scores providers against forty-eight criteria in eight weighted categories and assigns a level from SEAL-0 to SEAL-4. One criterion scores exposure to non-EU laws with cross-border reach, and the existence of legal, contractual or technical channels through which a non-EU authority could compel access.[1] The Commission scores jurisdiction directly rather than inferring it from a map, and a board can use the same criteria without buying anything.

The test is control, not location

The United States CLOUD Act reaches data in a provider's possession, custody or control, wherever it is stored. European subsidiaries of United States parents are in scope, as are European entities whose United States based staff can reach the data.[2] The statute does not require a provider to be able to decrypt, cannot be used for bulk collection, and allows comity objections where disclosure would breach foreign law.[2] It is a narrower instrument than the rhetoric suggests and a wider one than any residency clause can address.

Europe now has its own long reach. The e-Evidence Regulation has applied since 18 August 2026: a European Production Order can require subscriber, traffic and content data from any provider serving the Union, whatever its place of establishment, within ten days as standard and eight hours in an emergency, with penalties to two per cent of worldwide turnover.[3] A board that objects to extraterritorial compulsion in principle should note that its own continent now practises it.

The United Kingdom and United States agreement, in force since October 2022, expires on 3 October 2027 unless both governments renew it, and the traffic under it runs almost entirely one way: 20,142 orders sent by the United Kingdom to United States providers by October 2024, against 63 in the other direction.[4] That asymmetry is the practical shape of the dependency.

01 The duty
02 The data
03 The dependency
04 The evidence
05 The upside

ON THE RECORD

0

GUARANTEES

Asked in the French Senate for an assurance against disclosure to US authorities, June 2025: no, I cannot guarantee that.

The promises are real, and they stop short

The commitments made since 2025 are substantial and worth reading closely. Microsoft's sovereign options restrict remote access to personnel resident in Europe, record that access in a tamper evident ledger, and allow customers to hold keys in their own hardware modules; its European digital commitments are written into contracts with European governments, including an undertaking to contest in court any order to suspend cloud operations in Europe.[5] Amazon's European Sovereign Cloud launched in January 2026 with a German parent company, European leadership and the stated ability to keep operating indefinitely if cut off from the rest of the world.[6] Google commits to object to any suspension order by all available legal avenues, and states that its air gapped product cannot be remotely accessed or shut down by Google at all.[7]

Independent analysis puts the residual exposure where the statute puts it, at the corporate relationship rather than the address. The European entity remains a wholly owned subsidiary, and possession, custody or control turns on that relationship; customer held keys are the strongest technical mitigation, because the Act compels cooperation rather than decryption.[8] Assessments of the Microsoft offering reach the same place: the control plane stays globally integrated, and localisation does not remove the legal basis for access.[8]

The clearest statement on the record came under oath. Asked by the French Senate in June 2025 whether he could guarantee that French citizens' data would never be passed to United States authorities without French consent, Microsoft France's director of public and legal affairs answered that he could not, and added that it had never happened.[9] Both halves of that answer are useful. The first describes a capability. The second describes a history.

WHAT HAPPENED

1 **OVH**
Canadian production order served on the subsidiary, September 2025, reaching servers in three other countries.

2 **The ICC**
The prosecutor's account suspended, May 2025. The Court moved off the suite by October.

3 **Solvinity**
Dutch acquisition blocked, May 2026, on compelled access grounds.

Three things that have already happened

In September 2025 an Ontario judge refused OVH's application to revoke a production order requiring it to hand over account data tied to servers in France, the United Kingdom and Australia. The order was served on the Canadian subsidiary rather than routed through the mutual legal assistance treaty, leaving the company exposed to French criminal liability either way.[10] The compelling jurisdiction need not be the United States, and the subsidiary is the route.

In May 2025 the International Criminal Court prosecutor's Microsoft account was suspended after a United States executive order. Microsoft stated that its actions involved no cessation of services to the Court. The prosecutor moved to another provider, and by the end of October 2025 the Court was moving off the office suite entirely.[10] Continuity of service, not confidentiality, was the exposure that materialised.

In May 2026 the Dutch government blocked the acquisition of a domestic cloud provider by a United States buyer under its undesirable control legislation, on the ground that the ownership could expose national identity and government portal data to compelled access.[10] Ownership is now a regulated attribute of a supplier, not merely a commercial one.

THE OTHER DIRECTION

Art 32

DATA ACT

A third country order is enforceable in the Union only on the basis of an international agreement.

Europe has written its own rules on this

Article 32 of the Data Act makes a third country authority's decision enforceable in the Union only where it rests on an international agreement. Absent one, transfer is permitted only where the third country's system requires reasons and specificity, allows judicial review, and lets its courts weigh the interests Union law protects; providers must disclose the minimum permissible and tell the customer before complying, unless confidentiality is required for a law enforcement purpose.[11] The European

01 The duty
02 The data
03 The dependency
04 The evidence
05 The upside

Data Protection Board's final guidelines confirm that Article 48 of the General Data Protection Regulation is not itself a basis for transfer and that a foreign judgment has no automatic effect in the Union.[12] The supplier now sits between two legal systems, which is precisely where the board's risk sits.

Transatlantic adequacy is in force and survived its first challenge when the General Court dismissed the Latombe action in September 2025. An appeal to the Court of Justice was lodged that October and remains undecided, and the safeguards rest largely on executive orders that a later administration may alter.[13] Adequacy is current rather than settled, and a board should know what it would do in the fortnight after a judgment it did not want.

THE DISTINCTION

2

FACTS

Where the data sits, and who holds the entity. Suppliers answer the first when asked the second.

Five of these stay with the board

The technical mapping belongs to the executive. Five questions do not.

- **The jurisdiction map:** which data sets sit with which legal entity, under which law, and which could not be disclosed without serious consequence.
- **Key custody:** whether the organisation holds its own keys for what matters, and who inside the supplier can technically reach the plaintext.
- **The conflict of laws answer:** what each material supplier will do when two jurisdictions require opposite things, and whether that undertaking is contractual or promotional.
- **The never leaves list:** which categories must stay in a named jurisdiction, decided by the board rather than inferred by an architect.
- **The standstill plan:** how long the organisation could run from its own copy of its own data, and when that was last tested rather than described.

THE TEST

14

DAYS

The plan a board should have ready for the fortnight after an adequacy decision it did not want.

Ninety days of useful work

1. Commission a one page jurisdiction map: data set, holding entity, governing law, key custody, and who could compel disclosure.
2. Get each material supplier's conflict of laws undertaking in writing, and establish whether it sits in the contract or in a blog post.
3. Move key custody for the categories that matter, or record the board's decision not to, with reasons.
4. Score material suppliers against the Commission's published criteria rather than their own marketing, and ask which level they reach.
5. Test the standstill on one critical service, and put the result in front of the board with a date.
6. Put the question into procurement: require a sovereignty level and a conflict of laws undertaking at the next tender or renewal, rather than discovering both afterwards.

Sovereignty buys knowledge, not immunity

Sovereignty is not a promise that nobody can ever reach the data, but the ability to know who can, to make that a deliberate choice rather than an inherited one, and to keep operating when somebody exercises a power the organisation cannot prevent. Residency is geography. Compulsion follows jurisdiction. A board that understands the difference can price it; a board that does not will buy the map and believe it has bought the territory. None of the work above waits on the appeal in Luxembourg, on the next adequacy decision, or on the next European regulation. It waits on somebody being asked for the map.

01 The duty

02 The data

03 The dependency

04 The evidence

05 The upside

Twelve questions, and the answers that should worry you

Ask the executive	Worry if the answer is
Which legal entity holds our data, and under which law does it operate?	"It is stored in the EU." Location and holding entity are different facts.
Who inside the supplier can read our data in the clear?	"Nobody." Ask which roles can, in which countries, and how it is logged.
Do we hold our own encryption keys for the data that matters?	"The provider manages that for us." Then the provider can be compelled to act on the plaintext.
What will this supplier do if two jurisdictions require opposite things?	"They have committed publicly." Ask whether the commitment is in our contract.
Has this supplier ever been compelled to disclose data held in Europe?	"It has never happened." A claim about the past, not about capability.
What happens if this service is suspended for reasons unconnected to us?	"That would never happen." It happened to the ICC in 2025.
Which data must never leave a named jurisdiction, and who decided?	"Everything is classified appropriately." Ask for the list, and its board date.
How long could we operate from our own copy of our own data?	"We have backups." Backups held inside the same supplier do not answer this question.
What level would this supplier reach on the Commission's criteria?	"They are a sovereign cloud provider." The framework has levels. Ask which.
Does our AI processing follow the same rules as our data storage?	"The data stays in region." Ask where inference runs, and who operates it.
If adequacy were struck down, what would we do in the first fortnight?	"We would fall back on standard contractual clauses." Ask who has read them.
When did we last test any of this rather than read about it?	A reference to a supplier questionnaire. That is the supplier's homework, not ours.

NOTES AND SOURCES

1 European Commission, *Cloud Sovereignty Framework* v1.2.1, October 2025, criteria SOV-2 to SOV-4; applied in the Commission's own cloud award, 17 April 2026.

2 CMS, *The US CLOUD Act versus European data sovereignty*, 3 February 2026; Cross-Border Data Forum, CLOUD Act FAQs, July 2025.

3 Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 (e-Evidence), applicable 18 August 2026.

4 US Department of Justice, *Report to Congress on the US-UK CLOUD Act Agreement*, November 2024.

5 Microsoft, *Comprehensive sovereign solutions for European organisations*, 16 June 2025, and *One year on: our European digital commitments*, 29 April 2026.

6 Amazon, *AWS launches the AWS European Sovereign Cloud*, 15 January 2026.

7 Google Cloud, *Delivering a secure, open, sovereign digital world*, 7 February 2026.

8 Julien Simon, *Two sovereign clouds, one legal wall*, 26 February 2026, on the reach of 18 U.S.C. §2713; KuppingerCole, *Microsoft's sovereign cloud in 2026*, 20 April 2026.

9 Testimony of Anton Carniaux to the French Senate, 18 June 2025 (*The Register*, 25 July 2025).

10 Ontario Superior Court, OVH production order upheld 25 September 2025; JusticeInfo on the ICC, 19 March 2026; Jones Day on the Dutch decision of 25 May 2026.

11 Regulation (EU) 2023/2854 (Data Act), Article 32; applicable since 12 September 2025.

12 European Data Protection Board, Guidelines 02/2024 on Article 48 GDPR, final version adopted 4 June 2025.

13 General Court, Case T-553/23 *Latombe*, 3 September 2025; appeal lodged 31 October 2025, pending. Berkeley Technology Law Journal, 26 February 2026.

AltLibre Papers, board series, paper 02 of five. Adrian Hollister, AltLibre, 29 August 2026. altlibre.com Free to reuse with credit; not legal advice.