Digital sovereignty checklist for dealmakers

When you run private equity, M&A, real estate or financing deals, your most confidential information and deal communication sit on deal platforms. Digital sovereignty is about who ultimately controls that data – and which laws can force your platform provider to hand it over. One of the most important extra-territorial laws in this context is the US CLOUD Act.

What is the US CLOUD Act?

- The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is a US federal law enacted in 2018.
- It lets US authorities compel US electronic communications and cloud providers to disclose data, wherever it is stored in the world.
- It applies not only to US data, but to any data in the "possession, custody or control" of a provider under US jurisdiction.
- In June 2025, Microsoft France confirmed before the French Senate that they could ultimately hand over data stored in France if required by a US court order – a reminder that jurisdiction follows the provider, not just the server location.

Who is affected?

1. US-headquartered providers that own or store data (even in European data centres).
2. Non-US providers that are controlled by a US parent company or holding and therefore fall under US law.

The European platform for truly sovereign deals:

- Drooms is 100% European-owned and -controlled, HQs in Germany and Switzerland.
- All customer data is stored on georedundant servers in Europe.
- Core platform and AI features are developed in-house in Europe.
- Only European laws apply: Drooms is not subject to the US CLOUD Act..

More information on our security | Contact Sales

Digital sovereignty checklist for your next data room platform

Use this checklist in RFPs, procurement and internal risk reviews before you choose a deal platform.

A. Company and jurisdiction

- [ ] Is the company headquartered in Europe?
- [ ] Is the company fully European-owned and -controlled, without a non-European parent company or controlling investors?
- [ ] Is the company, or any parent entity, not subject to the US CLOUD Act?

B. Infrastructure and data location

- [ ] Will your data be stored and processed exclusively in Europe?
- [ ] Are all (if any) sub-processors for storing or processing your data located in Europe?
- [ ] Is all customer support, who can have access to data, delivered from within Europe?

C. Technology and AI

- [ ] Is the core platform technology (including AI features) developed in-house?
- [ ] Are integrated communication features governed only by European jurisdictions?
- [ ] Does the provider clearly specify where AI analysis services run (cloud and region)?
- [ ] Is your live data excluded from training the platform's AI by default?
- [ ] Is none of your data sent to public AI models?

D. Requests from foreign authorities

- [ ] Does the company have a documented process for handling government or law-enforcement requests from outside the Europe?
- [ ] Can the provider clearly explain how it would respond to a US order to share your data?
- [ ] Can the provider confirm it has never disclosed European-hosted customer data to non-European authorities?

E. Governance, certifications and contracts

- [ ] Is the provider certified under recognised security standards such as ISO 27001 / 27018?
- [ ] Is all data room activity logged, and can logs be exported for audits or legal proceedings?
- [ ] Does the platform offer detailed controls over access permissions, down to the document and user level?