

# Checklist sulla **sovranità digitale** per i responsabili delle operazioni

Quando gestisci operazioni di private equity, M&A, real estate o finanziamento, le informazioni più sensibili e le comunicazioni legate alla transazione vengono gestite attraverso piattaforme digitali dedicate. La sovranità digitale riguarda chi detiene, in ultima istanza, il controllo di questi dati e quali normative possono obbligare il provider della piattaforma a divulgarli. In questo contesto, una delle normative extraterritoriali più rilevanti è il CLOUD Act degli Stati Uniti.

## Che cos'è il CLOUD Act degli Stati Uniti?

- Il Clarifying Lawful Overseas Use of Data Act (CLOUD Act) è una legge federale statunitense entrata in vigore nel 2018.
- Consente alle autorità statunitensi di richiedere ai provider di servizi cloud e di comunicazione elettronica soggetti alla giurisdizione USA la consegna dei dati, indipendentemente dal luogo in cui sono archiviati.
- Si applica non solo ai dati localizzati negli Stati Uniti, ma a qualsiasi informazione sotto la "possessione, custodia o controllo" di un provider soggetto alla normativa statunitense.
- Nel giugno 2025, Microsoft France ha confermato davanti al Senato francese che potrebbe essere obbligata a consegnare dati archiviati in Francia su richiesta di un tribunale statunitense, evidenziando come la giurisdizione segua il provider e non esclusivamente la localizzazione dei server.

## A chi si applica?

1. Provider con sede negli Stati Uniti che archiviano o gestiscono dati, anche tramite data center situati in Europa.
2. Provider non statunitensi controllati da una società madre o holding americana e quindi soggetti alla legislazione USA.

## La piattaforma europea per operazioni realmente sovrane

- Drooms è una società interamente di proprietà e sotto il controllo europeo, con sedi in Germania e Svizzera.
- Tutti i dati dei clienti sono archiviati su infrastrutture georidondanti localizzate in Europa.
- La piattaforma e le funzionalità di intelligenza artificiale sono sviluppate internamente in Europa.
- Si applica esclusivamente la normativa europea: Drooms non è soggetta al CLOUD Act statunitense.

[Maggiori informazioni sulla sicurezza](#)[Contatta il team commerciale](#)

## Checklist sulla sovranità digitale per il tuo prossimo data room

Utilizza questa checklist nelle richieste di offerta (RFP), nei processi di procurement e nelle valutazioni interne del rischio prima di selezionare una piattaforma.

### A. Azienda e giurisdizione

- L'azienda ha sede in Europa?
- È interamente di proprietà e sotto controllo europeo, senza partecipazioni di controllo non europee?
- L'azienda — o la sua eventuale capogruppo — è esclusa dall'ambito di applicazione del CLOUD Act statunitense?

### B. Infrastruttura e ubicazione dei dati

- I dati vengono archiviati e trattati esclusivamente in Europa?
- Tutti i sub-responsabili del trattamento (se presenti) sono localizzati in Europa?
- Il servizio di assistenza clienti con potenziale accesso ai dati opera interamente dall'Europa?

### C. Tecnologia e IA

- La tecnologia core della piattaforma (incluse le funzionalità di IA) è sviluppata internamente?
- Le funzionalità di comunicazione integrate sono soggette esclusivamente a giurisdizioni europee?
- Il provider indica chiaramente dove vengono eseguiti i servizi di IA (infrastruttura e regione)?
- I dati in tempo reale sono esclusi per impostazione predefinita dall'addestramento dei modelli di IA?
- È garantito che i dati non vengano inviati a modelli di IA pubblici?

### D. Richieste da parte di autorità straniere

- L'azienda dispone di un processo documentato per gestire richieste da governi o autorità al di fuori dell'Europa?
- Il provider è in grado di spiegare chiaramente come risponderebbe a una richiesta delle autorità statunitensi?
- Può confermare di non aver mai condiviso dati di clienti ospitati in Europa con autorità non europee?

### E. Governance, certificazioni e contratti

- Il provider è certificato secondo standard di sicurezza riconosciuti (es. ISO 27001 / 27018)?
- Tutte le attività della data room sono tracciate e i log sono esportabili per audit o procedimenti legali?
- La piattaforma offre controlli granulari sui permessi di accesso, fino al livello di singolo documento e utente?