Checkliste zur digitalen Souveränität für Deal-Teams

Wenn Sie Transaktionen in den Bereichen Private Equity, M&A, Immobilien oder Finanzierung durchführen, liegen Ihre vertraulichsten Informationen und Kommunikation auf digitalen Transaktionsplattformen. Digitale Souveränität bedeutet, dass Sie die Kontrolle darüber behalten, wer auf diese Daten zugreifen darf – und welche Gesetze Ihren Plattformanbieter verpflichten könnten, sie herauszugeben. Eines der wichtigsten extraterritorialen Gesetze in diesem Zusammenhang ist der US CLOUD Act.

Was ist der US CLOUD Act?

- Der Clarifying Lawful Overseas Use of Data Act (CLOUD Act) ist ein US-Bundesgesetz, das 2018 verabschiedet wurde.
- Er ermöglicht US-Behörden, US-Anbieter von elektronischer Kommunikation und Cloud-Diensten zur Herausgabe von Daten zu verpflichten – unabhängig davon, wo diese weltweit gespeichert sind.
- Es gilt nicht nur für US-Daten, sondern für alle Daten, die sich im „Besitz, in der Verwahrung oder unter der Kontrolle“eines Anbieters unter US-Gerichtsbarkeit befinden.
- Im Juni 2025 bestätigte Microsoft France vor dem französischen Senat, dass das Unternehmen auch in Frankreich gespeicherte Daten herausgeben müsste, wenn dies per US-Gerichtsbeschluss angeordnet würde – ein klarer Hinweis darauf, dass sich die Zuständigkeit am Anbieter orientiert und nicht am Serverstandort.

Wer ist betroffen?

1. Anbieter mit Hauptsitz in den USA, die Daten die Daten besitzen oder speichern (auch wenn diese in europäischen Rechenzentren liegen).
2. Nicht-US-Anbieter, die von einer US-Muttergesellschaft oder -Holding kontrolliert werden und damit unter US-Recht fallen.

Die europäische Plattform für digitale Souveränität

- Drooms ist zu 100 % europäisch und unter europäischer Kontrolle, mit Hauptsitzen in Deutschland und der Schweiz.
- Kundendaten werden auf georedundanten Servern in Europa gespeichert.
- Die Kernplattform und die KI-Funktionen werden intern in Europa entwickelt.
- Es gelten ausschließlich europäische Gesetze: Drooms unterliegt nicht dem US CLOUD Act.

Weitere Informationen zu unserer Sicherheit

Kontakt zu Sales

Digitale Souveränität Checkliste für Ihre nächste Datenraum-Plattform

Nutzen Sie diese Checkliste für Ausschreibungen, Beschaffungsprozesse und interne Risikobewertungen, bevor Sie sich für eine Deal-Plattform entscheiden.

A. Unternehmen und Rechtsordnung

- [ ] Hat das Unternehmen seinen Hauptsitz in Europa?
- [ ] Befindet sich das Unternehmen vollständig in europäischem Besitz und unter europäischer Kontrolle, ohne nicht-europäische Muttergesellschaft oder beherrschende Investoren?
- [ ] Unterliegen weder das Unternehmen noch eine Muttergesellschaft dem US CLOUD Act?

B. Infrastruktur und Datenstandort

- [ ] Werden Ihre Daten ausschließlich in Europa gespeichert und verarbeitet?
- [ ] Befinden sich alle (sofern vorhanden) Subdienstleister für Speicherung oder Verarbeitung Ihrer Daten in Europa?
- [ ] Wird der gesamte Kundensupport, der potenziell Zugriff auf Daten hat, von Standorten innerhalb Europas erbracht?

C. Technologie und KI

- [ ] Wird die Kernplattformtechnologie (einschließlich KI-Funktionen) intern entwickelt?
- [ ] Unterliegen integrierte Kommunikationsfunktionen ausschließlich europäischem Recht?
- [ ] Gibt der Anbieter klar an, wo KI-Analysedienste ausgeführt werden (Cloud und Region)?
- [ ] Sind Ihre Live-Daten standardmäßig vom Training der Plattform-KI ausgeschlossen?
- [ ] Werden keine Ihrer Daten an öffentliche KI-Modelle übermittelt?

D. Anfragen von ausländischen Behörden

- [ ] Verfügt das Unternehmen über einen dokumentierten Prozess zum Umgang mit Anfragen von Regierungen oder Strafverfolgungsbehörden außerhalb Europas?
- [ ] Kann der Anbieter transparent darlegen, wie er auf eine US-Anordnung zur Herausgabe Ihrer Daten reagieren würde?
- [ ] Kann der Anbieter bestätigen, dass er niemals in Europa gehostete Kundendaten an außereuropäische Behörden weitergegeben hat?

E. Governance, Zertifizierungen und Verträge

- [ ] Ist der Anbieter nach anerkannten Sicherheitsstandards wie ISO 27001 / 27018 zertifiziert?
- [ ] Werden alle Aktivitäten im Datenraum protokolliert und können Protokolle für Audits oder Gerichtsverfahren exportiert werden?
- [ ] Bietet die Plattform granulare Kontrollmöglichkeiten für Zugriffsrechte bis hinunter auf Dokumenten- und Benutzerebene?