Digitale soevereiniteit checklist voor dealmakers

Uw meest vertrouwelijke informatie en deal communicatie bevindt zich op dealplatforms als u actief bent op het gebied van private equity, fusies en overnames, vastgoed of financiering. Digitale soevereiniteit gaat over wie uiteindelijk de controle heeft over die gegevens – en welke wetten uw platformaanbieder kunnen dwingen deze over te dragen. Een van de belangrijkste extraterritoriale wetten in deze context is de Amerikaanse CLOUD Act.

Wat is de Amerikaanse CLOUD Act?

- De Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is een Amerikaanse federale wet die in 2018 van kracht werd.
- Hierdoor kunnen Amerikaanse autoriteiten Amerikaanse aanbieders van elektronische communicatie en clouddiensten dwingen gegevens vrij te geven, waar ter wereld deze ook zijn opgeslagen.
- De wet is niet alleen van toepassing op Amerikaanse gegevens, maar op alle gegevens die zich in het "bezit, de bewaring of de controle" van een aanbieder onder Amerikaanse jurisdictie bevinden.
- In juni 2025 bevestigde Microsoft France voor de Franse Senaat dat zij uiteindelijk in Frankrijk opgeslagen gegevens zouden kunnen overdragen indien dit vereist werd door een Amerikaans gerechtelijk bevel – een herinnering dat de jurisdictie de provider volgt, niet alleen de serverlocatie.

Op wie heeft dit effect?

1. Providers met hoofdkantoren in de VS die gegevens bezitten of opslaan (zelfs in Europese datacenters).
2. Niet-Amerikaanse providers die worden gecontroleerd door een Amerikaanse moedermaatschappij of holding en daardoor onder de Amerikaanse wetgeving vallen.

Het Europese platform voor echt soevereine deals

- Drooms is voor 100% in Europese handen en wordt vanuit Duitsland en Zwitserland aangestuurd.
- Alle klantgegevens worden opgeslagen op georedundante servers in Europa.
- De kernfuncties van het platform en de AI-functies worden in eigen beheer in Europa ontwikkeld.
- Alleen Europese wetgeving is van toepassing: Drooms valt niet onder de Amerikaanse CLOUD Act.

Meer informatie over onze beveiliging | Neem contact op met sales

Digitale soevereiniteit checklist voor uw volgende dataroomplatform

Gebruik deze checklist bij offerteaanvragen, aanbestedingen en interne risicobeoordelingen voordat u een dealplatform kiest.

A. Bedrijf en rechtsgebied

- [ ] Is het hoofdkantoor van het bedrijf gevestigd in Europa?
- [ ] Is het bedrijf volledig in Europese handen en onder Europese zeggenschap, zonder een niet-Europese moedermaatschappij of controlerende investeerders?
- [ ] Is het bedrijf, of een moederentiteit, niet onderworpen aan de Amerikaanse CLOUD Act?

B. Infrastructuur en gegevenslocatie

- [ ] Worden uw gegevens uitsluitend in Europa opgeslagen en verwerkt?
- [ ] Zijn alle (eventuele) subverwerkers voor het opslaan of verwerken van uw gegevens gevestigd in Europa?
- [ ] Wordt alle klantenservice, die toegang kan hebben tot gegevens, vanuit Europa geleverd?

C. Technologie en AI

- [ ] Is de kerntechnologie van het platform (inclusief AI-functies) in eigen beheer ontwikkeld?
- [ ] Vallen geïntegreerde communicatiefuncties uitsluitend onder Europese jurisdicties?
- [ ] Geeft de aanbieder duidelijk aan waar AI-analysediensten worden uitgevoerd (cloud en regio)?
- [ ] Worden uw live gegevens standaard uitgesloten van het trainen van de AI van het platform?
- [ ] Worden uw gegevens niet naar openbare AI-modellen verzonden?

D. Verzoeken van buitenlandse autoriteiten

- [ ] Heeft het bedrijf een gedocumenteerd proces voor het afhandelen van verzoeken van overheden of wetshandhavingsinstanties van buiten Europa?
- [ ] Kan de aanbieder duidelijk uitleggen hoe hij zou reageren op een Amerikaans bevel om uw gegevens te delen?
- [ ] Kan de aanbieder bevestigen dat hij nooit in Europa gehoste klantgegevens heeft vrijgegeven aan niet-Europese autoriteiten?

E. Governance, certificeringen en contracten

- [ ] Is de aanbieder gecertificeerd volgens erkende beveiligingsnormen zoals ISO 27001 / 27018?
- [ ] Worden alle activiteiten in de dataroom geregistreerd en kunnen logbestanden worden geëxporteerd voor audits of juridische procedures?
- [ ] Biedt het platform gedetailleerde controle over toegangsrechten, tot op document- en gebruikersniveau?