DATA CENTER CHECKLIST

National Security & Cross-Border Risk

Foreign Investment, Data Sensitivity, and Geopolitical Considerations

HOW TO USE THIS CHECKLIST

This checklist is designed to help executive teams and in-house counsel identify and manage national security, cross-border, and geopolitical risks associated with data center ownership, operations, and expansion. It is not intended to be exhaustive or to provide legal advice but rather to highlight issues that can materially affect approvals, operational continuity, investment strategy, and regulatory compliance if not addressed early. The questions below are intended to support informed decision-making and coordinated planning across legal, infrastructure, finance, and operational teams.

WHO THIS IS FOR

CEOs, CFOs, GCs, boards, heads of infrastructure, and investment and strategy leaders responsible for domestic and cross-border data center projects, transactions, or operations.

01. Foreign Ownership, Control & Investment Exposure

- □ Does the ownership structure involve foreign investors, sponsors, lenders, or joint venture partners?
- □ Could the transaction or project trigger national security review or notification obligations?
- □ Are governance rights, access rights, or veto powers allocated in a way that raises control concerns?
- □ Are future changes in ownership or financing contemplated that could alter the risk profile?

WHY IT MATTERS:

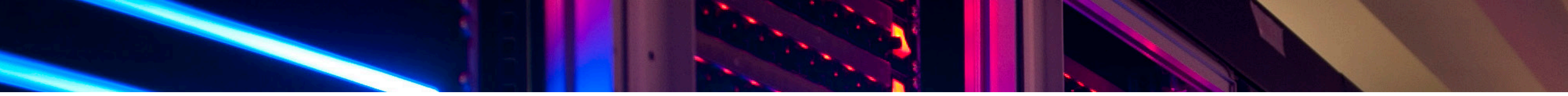
Foreign ownership or control can trigger regulatory review and impose conditions that affect operations and deal timing.

02. Sensitive Data & Workload Classification

- □ Are sensitive, regulated, or government-related workloads hosted or contemplated?
- □ Are data classification and segregation controls clearly defined?
- □ Are cross-border data flows identified and assessed?
- □ Are sovereign or localization requirements applicable?

WHY IT MATTERS:

The nature of hosted data can materially increase national security and regulatory scrutiny.



03. Location-Based National Security Risk

- □ Is the data center located near sensitive government, military, or critical infrastructure facilities?
- □ Could proximity raise security, surveillance, or access concerns?
- □ Are there location-specific restrictions affecting foreign access or control?
- □ Has location risk been evaluated independently of ownership structure?

WHY IT MATTERS:

Physical location alone can elevate national security risk, regardless of ownership.

04. Export Controls, Sanctions & Trade Restrictions

- □ Will U.S.-origin items, technology, or services be exported (either to build in a foreign geography or temporarily for testing or access for foreign vendors/employees)? If so, U.S.-origin hardware, software, or services should be reviewed to confirm applicable export controls or trade restrictions.
- □ Are vendors, customers, investors, or other counterparties subject to sanctions or embargoes? This may include list-based sanctions (e.g., the SDN list) or country-based sanctions (e.g., restrictions on transactions involving Russia, Iran, Cuba, etc.).
- □ Are compliance processes in place to monitor compliance with current applicable restrictions around sanctions and export controls and to identify and adapt to changes?
- □ Are contractual protections in place to require compliance by relevant third parties (e.g., vendors, investors, customers, and other counterparties) and to adapt to potential future changes in law (e.g., appropriate termination provisions)?

WHY IT MATTERS:

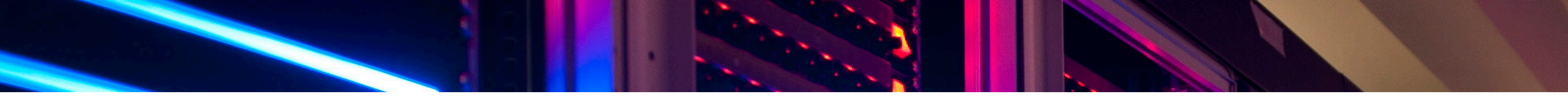
Trade and export restrictions can affect procurement, operations, investor, and other cross-border relationships, and these restrictions may change rapidly.

05. Government Access, Lawful Requests & Disclosure Obligations

- □ Are obligations to respond to government access or lawful requests understood?
- □ Are response protocols documented and tested?
- □ Are disclosure obligations to customers or partners clearly defined?
- □ Are cross-border conflicts of law identified?

WHY IT MATTERS:

Government access requests can create legal, reputational, and operational risk.



06. Cross-Border Operations & Regulatory Coordination

- ☐ Are operations, support services, or monitoring functions located outside the host jurisdiction?
- ☐ Are cross-border operational dependencies documented?
- ☐ Are regulatory regimes across jurisdictions aligned or in conflict?
- ☐ Are escalation and coordination mechanisms defined?

WHY IT MATTERS:

Cross-border operations increase complexity and exposure to conflicting legal obligations.

07. Transactional & Strategic Planning Considerations

- ☐ Have national security risks been assessed in M&A, financing, or joint venture planning?
- ☐ Are regulatory approval timelines aligned with transaction schedules?
- ☐ Are mitigation measures or conditions anticipated?
- ☐ Are exit and restructuring scenarios evaluated from a national security perspective?

WHY IT MATTERS:

National security review can materially affect deal certainty and valuation.

When To Call Us

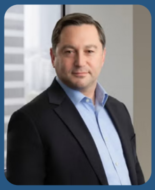
YOU SHOULD INVOLVE US EARLY IF:

- Foreign investment, financing, or joint ventures are contemplated
- Sensitive or regulated data will be hosted or processed
- The site is near government or critical infrastructure facilities
- Cross-border operations or support functions are involved
- Export controls or sanctions may affect investors, vendors, customers, or other cross-border counterparty relationships
- National security review (e.g., CIFIUS) could affect transaction timing or structure

We help clients assess national security risk, navigate cross-border regulatory frameworks, and structure data center projects and transactions to preserve deal certainty and operational continuity.

Authors:

Jamie Schafer
Partnerl | Washington, D.C.
JSchafer@perkinscoie.com



David Aaron
Senior Counsel | Washington, D.C.
DAaron@perkinscoie.com

For additional resources, visit: perkinscoie.com/datacenterhub.

Perkins Coie

Some jurisdictions in which Perkins Coie LLP practices law may require that this communication be designated as Advertising Materials.