The Rack Report | Q1 2026

Your inside look at what's powering tomorrow's data centers.

Perkins Coie

SPOTLIGHT INSIGHT

Tailoring Arbitration for Data Center Projects: Five Deal-Driven Essentials

by John Hardin

By any metric, data center construction is booming and is expected to continue doing so for the foreseeable future. Thousands of new facilities are projected to come online globally between 2025 and 2030, while total power capacity is expected to nearly double during that same period. The scale of capital deployment, technical complexity, and operational dependency is unprecedented.

In turn, data center contracts are often among the most complex and technically demanding agreements in modern infrastructure projects. They integrate construction, engineering, power procurement, cooling systems, commissioning, and ongoing operational performance into a single document. Dispute risk in this space rarely involves abstract breach issues. Instead, disputes often implicate uptime commitments, power availability, commissioning milestones, long-lead equipment delivery, and service-level credits owed to downstream customers. When those disputes arise, they are equally technical and carry significant operational and financial consequences for all involved.

Yet many data center contracts continue to rely on generic arbitration clauses recycled from unrelated projects or standard forms. For projects where downtime, delay, or misalignment can have outsized consequences, dispute resolution provisions deserve more intentional, deal-driven drafting commensurate with the project. Arbitration is a contract-driven resolution forum that can—and should—be tailored to the needs of the parties or the project. Below are five key considerations to begin those discussions.

1. How fast will your expected issues need to be resolved?
   Arbitrations often take time to initiate and provide meaningful access to decision-makers. But some data center disputes may require rapid resolution to protect operations.

   Arbitration clauses should be drafted with due consideration given to the most likely disputes that could arise and how quickly they must be resolved. Is emergency injunctive relief reasonably foreseeable? If so, do the selected arbitral rules adequately provide for expedited or injunctive relief, or will court intervention be required? Should certain categories of disputes be subject to accelerated timelines? Will interim relief be required to preserve operational continuity?

   For large-scale projects, would a dispute board, standing neutral, or structure escalation procedure be practical to resolve issues before they mature into full blown arbitrations?

2. What will be the technical complexity of a dispute?
   Data center disputes are frequently decided on technical evidence, yet generic arbitration clauses rarely account for this reality.

   What is the anticipated technical complexity of disputes related to the project? Should the parties agree in advance to baseline arbitrator qualifications? Do the anticipated arbitral rules adequately address expert-heavy proceedings, or should the parties supplement them to better accommodate engineering, scheduling, or systems-based evidence?

SPOTLIGHT INSIGHT (CONTINUED)

Tailoring arbitration for data center projects: Five deal-driven essentials

3. Do you want confidentiality or transparency?
   Confidentiality is often cited as a reason parties choose arbitration, but data center participants may have differing interests in how much information is protected—and from whom.

   Do the parties require strict confidentiality? Or would some degree of transparency be beneficial? Projects involving public companies, private equity sponsors, or project financing often require calibrated disclosure to investors, lenders, insurers, or, in some cases, regulators. Confidentiality obligations should be harmonized with those disclosure requirements rather than assumed.

   This baseline discussion should occur on all projects, so the dispute resolution clause reflects commercial reality instead of a one-size-fits-all assumption.

4. Does the arbitral seat and governing law provide the protection you need?
   Even when a data center project is located entirely within the United States, the parties, financing, or operational aspects may have cross-border elements.

   Does the chosen arbitral seat and governing law provide the enforceability, remedies, and procedural leverage best suited for the client or the project? For most domestic projects, a U.S.-seated arbitration governed by the laws of a U.S. state may be entirely appropriate. If foreign investors, international financing, or a global operator are involved, understanding the enforceability of an interim or final award abroad may materially affect leverage once a dispute arises.

5. Is your arbitration clause aligned with the commercial risk allocation in the contract?
   Arbitration clauses do not operate in isolation. They interact directly with the contract's allocation of risk, including limitations of liability, liquidated damages, insurance requirements, and force majeure provisions, and they should be considered holistically.

   Do the remedies available in arbitration align with the contract's negotiated limitations of liability and exclusive remedy provisions? Does the arbitration clause preserve the economic balance of risk allocated elsewhere in the agreement?

   If the dispute resolution framework allows for remedies or procedural mechanisms inconsistent with those negotiated risk allocations, the economic balance of the deal can shift in ways that were never intended.

Conclusion

Arbitration clauses in data center contracts should be treated as a strategic risk-management tool worthy of deal-intensive negotiations on par with other material provisions of the agreement. Tailoring the dispute resolution provision to the technical, operational, and commercial realities of the project can significantly influence how disputes are resolved and reduce their disruptiveness when they arise.

Legal and Regulatory Considerations for Data Center Development on Federal Land

by Kelly Doran, Laura Morton, Greg Vogel, Jessica Lockhart, and Madison Plummer

Building a data center on federal land introduces obligations and oversight mechanisms that often differ significantly from private sector development. On federal land, the federal government may retain ownership, regulatory authority, and inspection rights, which means that projects must often follow federal real estate, environmental, security, and compliance requirements throughout construction and operations.

Federal agencies may use several types of instruments to make land available for data center development. One common tool is the enhanced use lease (EUL), which allows agencies such as the Department of the Army to lease nonexcess property for long-term commercial development. Recent Army EUL solicitations indicate that these agreements can authorize developers to finance, construct, and operate data centers on military installations for terms up to 50 years. For example, an Army EUL at Fort Hood (now Fort Cavazos), Fort Bragg (now Fort Liberty), Fort Bliss, and Dugway Proving Ground illustrate typical federal requirements. Developers must conduct environmental reviews under the National Environmental Policy Act (NEPA), complete Environmental Condition of Property (ECP) reports, and comply with all applicable federal, state, and local laws throughout development and operations. These federal leases also provide agency inspection rights and require the developer to restore the land at the end of the lease term. These requirements differ from private sector ground leases, where inspection and restoration obligations are typically more limited.

Other agencies may also use traditional long-term leases, which rely on existing leasing authorities and allow them to select developers through competitive processes. In addition, energy-related property authorities may be used where a project provides onsite power or supports federal energy infrastructure goals, an approach encouraged by federal directives identifying priority federal sites for large-scale data center development, co-located with certain energy sources, including geothermal and nuclear energy. For example, the U.S. Department of Energy (DOE) has accelerated efforts to transform sections of its federal land portfolio into strategic hubs for AI-enabled data centers and advanced energy infrastructure by issuing four solicitations for data centers to be sited on DOE laboratory lands—Idaho National Laboratory, Paducah Gas Diffusion Plant, Oak Ridge National Laboratory, and the Savannah River Site.

But political priorities to site projects on these national laboratory lands do not mean data centers will be up and running as quickly as may be desired or projected. Multilayered, technology- and project-specific federal and state statutory and regulatory requirements still apply to constructing both data centers and the generation sources that power them on federal lands. Leases must be negotiated pursuant to DOE jurisdiction under the Atomic Energy Act (AEA) and the DOE Organization Act, which provide DOE with the authority to sell, lease, grant, and dispose of real property originally acquired in connection with AEA purposes. Like DOD, DOE must make decisions on the availability of the property following evaluations of mission need, land use plans, environmental conditions/status, potential environmental impacts, and the interests of the local community and tribes. Ultimately, when balanced against protection of the environment, water resources, cultural resources, and the interests of surrounding communities and tribes, developing on federal lands might be more difficult and time-consuming than necessary for the rapid growth of data centers and their power sources.

The federal government may also enter a direct contract to use the data center as an end customer. In these cases, the federal contract is governed by procurement regulations, such as the Federal Acquisition Regulation (FAR) and agency supplements like the Defense Acquisition Regulation Supplement (DFARS). Typical federal contracts include requirements related to information and physical security controls, such as the Cybersecurity Maturity Model Certification (CMMC), incident reporting, data handling, audit rights, and ongoing compliance with federal standards.

These traditional, FAR-based procurement contracts—as well as other common federal contract vehicles like grants, cooperative agreements, Other Transaction (OT) agreements, and Cooperative Research and Development Agreements (CRADAs)—may be used in whole or in part to build out a federal data center or aspects of a data center for federal use.

Federal contracts and agreements contain federal requirements that can create a broader risk environment for developers. Work performed on federal land or under federal agreements often involves detailed documentation, regulatory filings, and compliance certifications that the government relies on to monitor performance. For example, these agreements require representations that address a broad range of issues, such as certifying an entity's size status, prohibiting human trafficking, and safeguarding sensitive information. If information provided to the government is incomplete or inaccurate, developers may face increased scrutiny or enforcement action under federal fraud and compliance statutes, such as liability under the False Claims Act and suspension or debarment from federal contracting. This risk has become more pronounced following the U.S. Department of Justice's creation of the National Fraud Enforcement Division, which is focused on strengthening oversight of activities connected to federal program.

Fiber Rights: The Overlooked Utility in Data Center Deals

by Rachel Boyce

Did you know that one of the most critical—and often underestimated—"utilities" in a data center deal isn't water, power, or sewer, but the legal right to put fiber where you need it, when you need it? Securing long-haul and last-mile connectivity frequently turns on locking down easements, licenses, and rights-of-way early, aligning them with site control, and "future-proofing" route rights, so today's single-carrier path can scale into tomorrow's diverse, redundant network. This is where real estate and land use diligence earns its keep: mapping and recording corridor rights; synchronizing them with subdivision, title, and zoning milestones; and negotiating relocation and access provisions that keep projects moving even when routes change. In practice, one of the fastest ways to slow a build is to leave fiber rights until the end; one of the most effective ways to accelerate it is to treat connectivity rights like core "dirt" from day one.

Siting and Land Use—State and Community Engagement

by Laura Morton

Across the United States in 2025 and into 2026, community opposition to new data centers, particularly those tied to the AI infrastructure boom, has expanded well beyond traditional tech regions, with grassroots resistance taking hold from Georgia and Texas to Arizona, Wisconsin, Michigan, California, and beyond. Residents in Georgia counties have pushed for temporary pauses on new approvals to evaluate local impacts, while grassroots campaigns in Arizona cities helped city councils unanimously reject major AI data center proposals amid water, energy, and quality-of-life concerns. In Texas, cities are witnessing tense public debates over proposed data center campuses as neighbors cite water usage, noise, and environmental impacts in heated council meetings. Elsewhere, community groups have successfully halted construction and spurred temporary moratoriums after mobilizing large petitions and public pressures—part of a broader pattern of local resistance blocking or delaying billions in proposed projects nationwide.

In response to rising public and legislative scrutiny, a growing number of state and local governments also have introduced moratoriums or proposed temporary halts on data center development in 2025-2026 to buy time for studies, permitting reforms, and new regulatory frameworks. Moratoriums are typically framed as temporary "study periods"—ranging from 45 days to one year—intended to allow planning commissions to draft or revise ordinances addressing setbacks, noise from backup generators, substation placement, transmission upgrades, traffic during construction, and cost allocation for grid improvements.

Legislators in states such as Georgia have proposed statewide moratorium bills slated to pause approvals until officials can set policies for regulating facilities across energy, water, and land use. New York lawmakers introduced a three-year moratorium bill that would require environmental and social impact assessments before new data centers can be approved. In Vermont, lawmakers have introduced legislation that would impose a statewide moratorium on AI data centers through 2030, while regulators study impacts on utilities and ratepayers. In Maryland, proposed legislation would prohibit new data center construction statewide pending further evaluation of energy, land use, and environmental considerations. Additional moratorium proposals are advancing in Oklahoma, where a multiyear pause has been filed to study long-term effects, and in Virginia, where a temporary halt in approvals is under consideration as part of a broader package of data center-related legislative efforts.

A significant number of local governments have enacted temporary moratoriums or development pauses on new data centers, particularly in Michigan, but also in Georgia, Kansas, Wisconsin, Indiana, North Carolina, California, and Idaho, largely in response to the rapid scale and pace of hyperscale and AI-driven facility proposals. In some cases, local officials have adopted moratoriums. For example, Chatham County, North Carolina, and Meade County, Kentucky, adopted yearlong pauses to reassess zoning and infrastructure capacity, and Monterey Park, California, enacted a 45-day interim moratorium to study land-use impacts. In Kootenai County, Idaho, commissioners enacted an emergency moratorium to address gaps in zoning and permitting, and multiple Michigan townships did likewise to update local ordinances.

In states like Michigan and Kansas, clusters of multiple township-level moratoriums—including actions in Sedgwick County, Kansas, and Marion County, Kansas—reflect localized reactions to specific proposed projects that triggered community pushback over land-use compatibility and perceived disproportionate impacts on rural communities.

Elsewhere, such as in parts of Wisconsin, Georgia, Indiana, North Carolina, Idaho, and California, local pauses have similarly been justified as necessary to evaluate long-term infrastructure strain, environmental review requirements, water availability, and whether large-scale data centers align with local economic development priorities. In short, these temporary moratoriums are not outright bans but regulatory “time-outs” aimed at recalibrating land-use frameworks to address the unique scale, utility intensity, and community impacts of modern data center development.

In other jurisdictions, proposed moratoriums were rejected or not adopted. For instance, in Hood County, Texas, commissioners twice declined to impose a pause on data center applications after legal concerns about authority were raised, and in parts of Maryland, local debates around zoning and utility impacts have occurred without formal moratorium ordinances to date. In South Carolina, several counties have discussed pauses, but no county-level moratorium has yet been widely reported. Proposed state legislation would preemptively pause permits if enacted.

This wave of moratorium initiatives reflects an emerging trend in which policymakers at multiple levels seek to balance economic development with concerns over infrastructure strain, environmental impacts, and community priorities. Developers should anticipate heightened scrutiny, potential mid-process regulatory changes, and increased entitlement risk. The key to success is early engagement, transparency, open and broad communication, partnership, and solutions that fit communities.

Land Use and Site Selection for Data Centers: From Zoning to Powered Land Deals

by Camarin Madigan, Anne Li, and Megan Lin

Land use is often an early hurdle in data center development. Data center projects can require a wide range of land use approvals, and the level of public participation, scope of review, and timeline for issuance depends heavily on location. A critical first step is understanding the local general plan and zoning ordinance to determine whether data centers are permitted outright or with some form of administrative, conditional, special use, or similar use permit. If not—or if the use is not contemplated at all—the entitlement process will be longer and more complex, potentially requiring a legislative text amendment or a rezone. Developers should also consider whether related infrastructure, such as substations, switching stations, or other necessary onsite utility infrastructure, are allowed as an independent or accessory use. In general, industrial zones are more likely to permit data centers and related infrastructure. Next, it is equally critical to evaluate whether there are other restrictions—like master plans, zoning overlays, critical areas, and shorelines and buffers—that could affect development of the site. Finally, developers should consider whether offsite utilities and road infrastructure must be improved or extended to serve the development (and the feasibility and costs of such improvements) and confirm conformance with onsite development standards, such as setbacks, height restrictions, separation from sensitive uses (like residential neighborhoods or schools), local noise ordinances, design review, and parking and landscaping requirements. These last considerations are usually not an outright bar to development but can impact project design, costs, and timelines.

How Data Center Site Selection is Evolving

In past years, many developers and hyperscalers followed a land-banking model—acquiring property first and planning to secure power, construct the facility, and procure racks and equipment later. More recently, there's been a rise in "powered land" deals, where site control and committed power are acquired together. In some cases, intermediaries take options on land and coordinate interconnection approvals in advance, aiming for a back-to-back closing between the land option and the ultimate sale to the data center developer—with power effectively bundled into the transaction. However, supply chain delays and long interconnection queues continue to change structure and timing of deals. Today, developers are often ordering critical equipment before they've even finalized a site. That shift requires more flexible contract terms—allowing delivery to multiple potential locations or temporary storage while power and land are secured.

Navigating the AI-Driven DRAM Shortage: Critical Contract Terms for Supply Chain Resilience

by Chris Wieman

There is a global AI-driven shortage of dynamic random-access memory (DRAM) that is expected to last at least through 2028. Shortages of one kind or another are likely the "new normal" as infrastructure demand, geopolitical risk, and other supply chain bottlenecks are likely to create new, and deepen existing, shortages of critical components in the years ahead.

When negotiating strategic supply agreements, it is critical for buyers to put in place mechanisms and supplier obligations that will improve continuity of services and limit operational disruption when one of these shortages occurs and for suppliers to preserve flexibility, so they do not face outsized risk from force majeure events. For purchasers, provisions related to buffer inventory requirements, reserve capacity, and MFNs are all critical tools to accomplish this goal. Beyond the contract, parties should also implement operational processes to reduce supply chain risk and address issues such as sole sourcing, tariffs, and rare earth restrictions. The appropriate strategies will vary depending on the availability of supply, liquidity, and relative leverage of the parties. It is important to consider external disruptions and resource restrictions when you are negotiating supply agreements and planning your supply chain strategy.

Five Critical Decisions for Data Center Power Projects: From Delivery Model to Commissioning

by Kevin Kolton

Data centers need power that is fast, clean, and predictable during defined critical windows. When onsite or adjacent generation supports IT load, sponsors and EPCs face five decisions that directly affect uptime:

1. choosing the right delivery model—single engineering, procurement, and construction (ECP) vs. engineering, procurement, and construction management (EPCM)[1]—with disciplined interfaces;

2. demanding guarantees that go beyond nameplate to cover availability during critical windows, start/response times, and point of common coupling (PCC) power quality (total harmonic distortion (THD), flicker, voltage ride-through);

3. maintaining schedule integrity by treating utility reviews, witness tests, and long-lead procurement as true critical path;

4. (implementing pragmatic operational technology (OT) security baselines that segment controls, enforce access, and align patching and incident service level agreements (SLAs) with original equipment manufacturer (OEM) obligations; and

5. managing change without stall through hybrid pricing, pre-agreed triggers, and rapid-response protocols that keep crews moving while commercials finalize.

The practical takeaway: Define “critical windows” early, measure power quality at the PCC, front-load utility engagement, make security operable, and treat the interface matrix as a living artifact. These steps ensure capacity shows up exactly when IT workloads need it.

With the EPCM model, the contractor (or an integrator) manages and coordinates engineering, procurement, and construction activities, but the owner holds the prime contracts with key vendors and trades. The practical implications are more owner control and flexibility, but higher interface risk unless you define a disciplined integrator role, clear responsibility assignment RACI, and strong interface/commissioning protocols.