BCLP. Client Intelligent

Insights

STRUCTURING THE NEXT GENERATION OF DATA CENTRE TENANT AGREEMENTS

DATA SOVEREIGNTY, SECURITY AND AI

Feb 24, 2026

For years, the conversation around data centres has focused on physical assets: power, land, water and concrete. But as the world moves deeper into a new era defined by geopolitical tension and the explosive rise of artificial intelligence (AI), the real strategic value of these facilities lies in the data they store and process. Increasingly, data centres form part of a global information supply chain in which legal jurisdiction, regulatory exposure and operational resilience carry as much weight as physical infrastructure.

For developers, investors and hyperscalers, this shift demands a recalibration. The legal and regulatory architecture surrounding a data centre – once treated as a secondary concern – is now a primary determinant of asset value, risk allocation and long-term viability. The challenge for market participants is to navigate a rapidly evolving landscape of data sovereignty rules, intensifying security expectations and the operational demands of AI-driven computing.

THE GEOPOLITICS OF DATA: NAVIGATING SOVEREIGNTY AND CROSS-BORDER TRANSFERS

The internet was originally conceived as a borderless space, unconstrained by geography and largely indifferent to national boundaries. That vision has steadily eroded. Today, digital nationalism is reshaping the global data landscape as governments assert sovereign control over the information generated within their borders. For multinational companies and the data centres that support them, this shift has created a complex and often fragmented regulatory environment.

In Europe and the UK, the legacy of the Schrems II decision, which invalidated the EU-US Privacy Shield, continues to cast a long shadow over transatlantic data flows. The subsequent EU-US Data Privacy Framework and the UK-US “data bridge” offer a route forward, but their stability remains uncertain; both could face further legal or political challenges. As a result, many tenants are adopting conservative “data residency” strategies, ensuring that EU and UK personal data is stored and processed exclusively within domestic facilities wherever possible. This trend is increasingly

shaping data centre site selection, driving demand for high-quality capacity in key European and UK markets.

For developers and operators, the ability to support these residency requirements has become a significant commercial differentiator. Lease and colocation agreements now routinely incorporate enhanced tenant protections, including rights to audit data location, landlord warranties confirming that operational data remains within the jurisdiction, and clear protocols for handling law-enforcement requests. Tenants are no longer only looking for compliance, but also clear contractual assurance.

The regulatory challenge, however, is global. Countries from India to Brazil are introducing their own localisation regimes, creating a patchwork of rules that investors and operators must navigate. For those managing multi-jurisdictional portfolios, strategic decision-making now hinges on understanding this evolving mosaic and anticipating how it will influence both asset deployment and long-term operational risk.

THE AI IMPERATIVE: RISING SECURITY AND OPERATIONAL DEMANDS

The rise of generative AI has triggered a step-change in the demands placed upon data centres. The immense computational power required to train and run large language models (LLMs) is reshaping not only the power and cooling requirements of these facilities, but also their security and operational protocols.

As ever more processing power and proprietary AI models are concentrated within single sites, data centres have taken on a new level of strategic significance. This is driving a marked escalation in physical security requirements. Lease and colocation agreements now contain highly detailed security protocols, often as a dedicated schedule. These go far beyond standard access controls, specifying requirements for multi-layered security zones, advanced biometric authentication, anti-climb perimeter fencing, vehicle crash barriers and sophisticated 24/7 surveillance systems with advanced threat detection analytics. The landlord's ability to deliver and maintain this type of "fortress-grade" security is a critical factor in attracting and retaining AI-focused tenants.

The bar for operational resilience is rising just as sharply. For an AI platform, downtime is not just an inconvenience; it can result in catastrophic financial and reputational damage. As a result, the Service Level Agreement (SLA), which is typically a schedule or annex to the lease or colocation agreement, has become one of the most heavily negotiated documents. The traditional "five nines" (99.999%) uptime guarantee for power and cooling is now the absolute minimum standard. Sophisticated SLAs for AI tenants include granular performance metrics for power quality (voltage and frequency stability), humidity and temperature tolerances within the data hall, and the response times for the landlord's engineering teams.

The financial penalties for breaching these SLAs, known as "service credits", are also increasing in scale, reflecting the immense value of the computational work being undertaken. These developments also bring questions of liability into sharper focus. The deployment of powerful AI systems requires a clear allocation of responsibility between the operator and the tenant. While the landlord is responsible for the physical environment and the core infrastructure, the tenant remains responsible for the security and operation of its own servers and the AI models running on them. The associated provisions within the lease or colocation agreement are therefore critical. They must be carefully drafted to ensure that each party takes responsibility and liability for losses arising from its own sphere of responsibility.

THE EVOLUTION OF THE DATA CENTRE AGREEMENT: A NEW CONTRACTUAL PARADIGM

The convergence of data sovereignty, security and AI is forcing a fundamental evolution in the legal agreements that govern the relationship between data centre landlords and tenants. The traditional property lease or colocation agreement is being transformed into a hybrid document – part real estate contract, part technology service agreement – reflecting the far broader responsibilities now carried by operators.

One notable development is the growing use of Master Services Agreement (MSA) structures, particularly for tenants deploying capacity across multiple sites and jurisdictions. Under this model, the core commercial and legal terms – covering areas such as liability allocation, data protection obligations and security standards – are set out in a single overarching agreement. The site-specific details are then documented in separate site or service orders that sit below the MSA. This structure provides greater flexibility and efficiency, allowing the parties to quickly deploy new capacity in different locations without having to renegotiate the entire legal framework each time.

Futureproofing has also become a central concern. This is because the pace of technological change means that a data centre built today may need to accommodate technologies that don't yet exist. The lease or colocation agreement must therefore be a dynamic document, capable of adapting to this evolution. This involves incorporating "technology-proofing" clauses. For example, the agreement may include provisions that allow the tenant to install next-generation cooling systems (such as direct-to-chip liquid cooling) or to draw down significantly higher power densities in the future, subject to a clear commercial framework for sharing the costs of any necessary upgrades to the base building infrastructure.

STRUCTURING FOR A DATA-CENTRIC FUTURE

The resilience of a data centre depends not only on generators, steel and concrete, but on the contractual architecture that determines how data is governed, secured and controlled. As digital borders intensify and AI amplifies both opportunity and risk, these agreements have become strategically critical. We are moving towards a world in which the most competitive operators are

not just those with the largest power reserves, but those able to navigate the interlocking demands of regulation, security and technology. The firms that succeed will be those that treat the contract not as an administrative formality, but as a core component of the infrastructure itself.

HOW WE CAN HELP

Advising on data centre agreements now demands a rare combination of disciplines: deep property expertise, a detailed understanding of global data regulation and an appreciation of the operational pressures created by AI-driven infrastructure. The work increasingly involves aligning these strands into contracts that are commercially bankable, technically realistic and resilient to regulatory change.

Our integrated global team works with clients to structure agreements that provide tenants with certainty over security, data governance and operational performance, while allowing developers and operators to deliver these obligations efficiently across multi-site portfolios. This includes crafting flexible contractual frameworks that can accommodate rapid deployment in different jurisdictions without reopening core legal terms. We also advise on future-proofing agreements to allow emerging technologies and higher operational demands, and on allocating liability across complex AI and infrastructure operations.

Combining legal, technical and regulatory insight, we help clients create data centre contracts that are not only compliant and secure, but robust enough to adapt as the market and technology continue to evolve.

Related articles

Regulatory and ESG challenges in the data centre sector: Building a sustainable future

Unlocking Value in UK Data Centre M&A Transactions

Financing data centre developments: Balancing risk and opportunity in a capital-intensive sector

RELATED CAPABILITIES

- Data Centers & Digital Infrastructure
- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

Partner and EMEA Lead of Data Privacy and Security, London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Benjamin Wheeler

Partner, London

benjamin.wheeler@bclplaw.com
+44 (0) 20 3400 3407
