

Insights

DATA CENTRE INVESTMENT IN THE UK: IF YOU BUILD IT, WILL THEY COME?

Jul 20, 2026

Summary

What do you think about when you think about data centres, particularly in the context of the UK government's commitment to regulate for growth and harness the efficiencies promised by AI innovation? We saw in the recent [King's Speech](#) clear signs the government recognises the essential nature of the services a data centre provides (and its concomitant desire to protect those businesses who rely on data centre services). And with all the talk of token use and the raw compute power required to support the UK's rapidly increasing adoption of AI, what challenges does the data centres industry face in the UK and how does it keep pace with the increasing levels of demand?

Regulatory changes

Critical regulatory changes are afoot, which were first set out in the UK's proposal for a Cyber Security and Resilience Bill in November 2025 (discussed in more detail in our [insight](#)). This remains part of the government's regulatory agenda, as set out in the May 2026 [King's Speech](#). The Bill will ultimately bring data centres within the scope of the UK's Network and Information Systems Regulations as these are seen as "*critical to keeping the UK running, underpinning essential and digital services from patient records and online payments to email services and AI development.*"

The Bill will require in-scope entities to report a greater range of cyber incidents to their regulator and the National Cyber Security Centre (NCSC) within 24 hours, followed by a full report within 72 hours. This will help entities access national cyber security resources and enable systemic threats to be logged quickly, protecting the wider economy from threats that could spread rapidly across interlinked systems. Data centres facing a significant cyber incident will also need to promptly notify affected customers, enabling them to act fast to limit the impact on their business, people and services. The government is reinforcing the importance it places on implementation of robust

cyber security measures, with the introduction of turnover-based penalties for serious breaches "*so cutting corners is no longer cheaper than doing the right thing.*"

So, what will this require of data centre operators? In practice, it means rigorous cyber security measures, robust business continuity plans, active board-level oversight and reliable horizon scanning to ensure defences keep pace with increasingly AI-assisted cyber criminals and the interdependence of key systems on the largest tech providers. According to a report by IBM, the UK is the most targeted country for cyber attacks in Europe. In addition, a 2025 KPMG report estimated that a systemic cyber incident to the rail network causing one week of disruption could result in an estimated cost of £1.8 billion. Recognising the threat posed, the government will be strengthening cyber regulators to ensure they are more effective in their efforts to protect essential services, with companies who provide essential services required to have "*tough protections*" to keep their systems and operations running.

The EU dimension: digital sovereignty and data centre expansion

The UK's regulatory environment for data centres must also be seen in the light of the EU's ambitions to bolster the EU's digital autonomy and reduce reliance on non-EU suppliers. The EU recently announced measures to strengthen its capabilities in semiconductors, AI, cloud computing and open source technologies and establish a sovereign cloud and AI offer in the EU. This will involve two key legislative initiatives: (i) the Chips Act 2.0, which will expand semiconductor capacity (particularly building capacity in cutting-edge semiconductor technologies that power AI applications), support investment and strategic projects and address supply chain vulnerabilities; and (ii) the Cloud and AI Development Act (CAIDA). CAIDA aims to triple data centre capacity within five to seven years, support the deployment of cloud and AI technologies, strengthen the EU's Apply AI strategy and establish an EU-wide framework for assessing cloud and AI sovereignty. It also forms part of the AI Continent Action Plan. The stated ambition is to streamline conditions for deploying data centres across the EU, with a focus on highly sustainable and innovative facilities at the scale needed for the green and digital twin transition. It will also introduce a single EU-wide framework to assess cloud and AI sovereignty, while keeping 'most' of the EU market open to like-minded partners. It is clear there is an impetus to protect critical applications and sensitive data, and support the development and roll-out of advanced EU cloud and AI technologies.

As part of the CAIDA objectives, each EU Member State would need to designate at least one data centre acceleration zone. The EU would be able to designate certain data centre projects as 'strategic projects' where a centre supports essential public infrastructure, includes highly sustainable or innovative features, supports the electricity grid or another advanced technology such as quantum computing or addresses a major shortage of compute capacity. CAIDA also sets out EU assurance levels for cloud providers based in the EU (as well as for non-EU cloud providers). Non-EU providers would need to ensure that they are not subject to national legislative measures which would: (i) compel the provider to degrade or disrupt service continuity or provision; (ii) oblige

the provider to implement / give effect to restrictive measures such as sanction regimes, embargoes; (iii) impede the provision of state-of-the-art technologies and services provided by the provider; (iv) it maintains an open market to EU cloud computing services.

These key strategic objectives are to be supported by the Open Source Strategy (which seeks to scale up open-source alternatives in cloud, AI, cybersecurity and semiconductors, strengthen the open-source ecosystem and increase their use in public administrations) and the Strategic Roadmap for Digitalization and AI in the Energy Sector. This latter initiative aims to support the sustainable integration of digital infrastructure into the energy system, accelerate the deployment of digital and AI solutions and improve the efficiency of Europe's electricity infrastructure.

Balancing investment with regulatory complexity

The King's Speech also recognised the UK's drive to attract investment, particularly in the realm of AI, which contributed an estimated £11.8 billion to UK GDP in 2025, with over £1 billion in venture funding raised in just the first quarter. However, there are also concerns that the increasing regulatory burden risks deterring investment; the King's Speech [noted](#) that nearly one third of UK AI startup leaders are considering relocating overseas due to regulatory complexity and capital constraints.

Building on the foundations of the 2025 Regulation Action Plan, the government has indicated that it needs to balance the competing objectives of promoting growth whilst also safeguarding vital national interests, by ensuring regulation keeps pace with the unprecedented speed of technological innovation. Inspired by measures adopted in Singapore and Canada, it wants to enable rapid but controlled testing of new approaches through regulatory sandboxes, followed by the swift rollout of reforms, to enable the UK *"to safely seize opportunities, from artificial intelligence (AI) and other emerging technologies to breakthrough medical advances – to the benefit of UK businesses, citizens and national security."*

Pace of technological change

The sustained pace of change we see means the threats posed are magnified, with a new generation of AI models increasingly capable of taking hostile action, finding and exploiting weaknesses in software at speed and scale, as we see with the AI Security Institute's testing of Mythos, which has substantially increased attacking capabilities.

But the technology to support the large models also relies on cutting edge chip technology and sophisticated data centre technology. To avoid data centres becoming data sheds or stranded assets, operators need to be able to retrofit at speed, enabling centres to operate at scale and offer sufficient compute power for current and projected need.

Environmental factors

Recent headlines underscore data centres' dependence on electricity suppliers, the attendant risk of energy shortages in the UK, and their growing environmental footprint. The International Data Center Authority estimates that data centres now consume 6% of electricity in the UK and US, with global energy use rising 15% over the past two years. In the first half of 2025 alone, the queue to connect to the grid grew by 460%.

Data centres also face increasing scrutiny over their water consumption and cooling requirements. Traditional cooling systems are water-intensive, and as facilities scale to meet AI-driven demand, the strain on local water resources is becoming a material planning and environmental concern. Operators are under growing pressure to adopt innovative cooling technologies, including liquid cooling, immersive cooling and waste heat recovery not just to deal with the heat generated by AI workflows, but also to demonstrate measurable progress on sustainability commitments for both regulators and investors.

Labour market

Underpinning all of this is the quality and depth of the UK's labour market. While the UK has established strengths in engineering, cyber security and digital infrastructure, skills shortages in these areas remain acute and competition for qualified professionals is fierce. Attracting and retaining the workforce needed to design, build and operate the next generation of data centres, while also meeting the heightened compliance demands of the incoming regulatory framework, will be a defining challenge for the sector.

Summary

The cyber security sector itself makes an important economic contribution to the UK, generating £13.2 billion in revenue in 2024 alone, employing 67,300 people and creating 6,600 new jobs in the year to 2025. These figures illustrate both the scale of the opportunity and the depth of capability the UK can draw on as it seeks to position itself as a global leader in secure, sustainable digital infrastructure.

The trajectory is clear - data centres are now clearly recognised as critical national infrastructure, and the regulatory, environmental and technological pressures on operators will only intensify. Those who invest early in robust cyber resilience, sustainable operations and workforce development will be best placed to capture the significant growth opportunities ahead and to meet the expectations of UK government, regulators and customers alike.

BCLP is uniquely positioned to help clients navigate these challenges. With unrivalled expertise across the full data centre sector, we advise investors, developers, operators and users at every stage: from site acquisition and planning, energy procurement through construction and financing, to operational compliance and commercial contracts, drawing on subject matter experts across our practice areas to deliver seamless, globally coordinated support. If you would like to discuss

any of the issues raised in this article, or how we can support your data centre business, please do not hesitate to contact any member of our team.

Related Capabilities

- Digital Transformation & Emerging Technology
- Technology Transactions
- Data Centers

Meet The Team



Benjamin Wheeler

Partner, London

benjamin.wheeler@bclplaw.com

[+44 \(0\) 20 3400 3407](tel:+442034003407)



Anna Blest

Knowledge & Innovation Counsel,
London

anna.blest@bclplaw.com

[+44 \(0\) 20 3400 4475](tel:+442034004475)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.