Thought leadership

Strategic AI infrastructure: building, regulating and monetising the future

Clifford Chance

November 2025

Strategic AI infrastructure: building, regulating and monetising the future

Key takeaways

1. Be clear about the strategic opportunities the business intends to monetise or obtain business advantage from and the countries/regions of focus
2. Work with your business teams and your lawyers to understand the international trade and regulatory landscapes in those markets to ensure compliance and flexibility is built into the business model
3. Consider your contracting approach. Well thought through contracts can be invaluable in dealing with business and regulatory uncertainty and change as well as supply chain resilience

As AI accelerates, so does the need for infrastructure that can keep pace. From high-density compute and advanced cooling for AI data centres to AI factories that transform raw data into intelligence, the backbone for AI processing is being built out at speed. In this extract from a recent webinar, we explore some of the key regulatory considerations which may affect decision-making around where to locate, use and/or monetise AI, AI data centres and AI factories, focusing on trade and tariffs, competition, foreign investment, data and data sovereignty. We also consider how government policy and regulation can shape choices for those investing in, building, monetising or using AI, AI factories and the underlying software, hardware and services.

What do we mean by "AI-ready data centres" and "AI factories"?

At the backbone of our digital world, data centres are pivotal, empowering a wide range of technological and digital services that are fundamental to society and business operations. Whilst traditional data centres can support some AI workloads, AI factories operating at scale benefit significantly from specialised data centres designed to meet the unique demands of AI operations.

AI-ready data centres are specialised facilities built to meet the distinctive demands of AI, combining high-density GPU or TPU clusters, robust power, advanced (increasingly liquid) cooling, high-speed networking and high-throughput storage, and they are defined as much by site constraints as by compute. On top of this physical layer, AI factories add the operational and software stack that turns capacity into output, providing end-to-end environments to develop, train, fine-tune, evaluate and deploy AI models at scale with tight integration across hardware, software, data governance and operations.

A growing trend in this space are Gigawatt campuses, being data centre facilities designed to deliver 1 GW or more of power capacity, purpose-built for AI workloads. These are not just larger versions of traditional data centres – they are AI-first infrastructures optimised for the unique needs and challenges of building infrastructure to support the volatile workloads of AI.

The combination of the changing technology profile required for AI-ready data centres and AI factories; the availability of materials/hardware and consequential skills requirements to optimise the opportunity; together with some of the regulatory challenges businesses face in this space has direct consequences for site selection, construction standards, operating procedures and approach to acquisition or usage, as well as in relation to any underlying contracts.

Why this matters now

Global spend on AI-capable infrastructure is accelerating and a significant share of new data-centre investment is being redirected to AI workloads. Gartner projects that, by 2027, AI-related infrastructure will account for 30 to 40 per cent of all new data centre spending. Unsurprisingly, the US and China are at the forefront of investment, with both regions investing billions of dollars in new and upgraded data centres specifically designed for AI workloads. The EU has also already spent over US$10 billion in this space.

"Wherever your business or entity sits in this AI ecosystem, the opportunity is clear. With such potential to monetise this technological shift, we are seeing huge investment and work in this area," says Charlotte Walker-Osborn, a Knowledge Director in Clifford Chance's Tech Group. "However, set against this backdrop are geopolitical and legal hurdles to understand and navigate at the right time."

Location and permitting choices have become strategic because of power availability, water usage, networking infrastructure and local community impact. Compliance, cyber and national security and geopolitics sit side by side. Data protection, cybersecurity, export control and foreign-investment screening and other regulatory, sectoral and planning considerations are now part of core business planning rather than afterthoughts, as is building flexibility into contracts.

So, what should businesses do? It is quite helpful to approach thinking about AI infrastructure and AI factories a bit like one would approach a regulated industrial platform rather than simply as more data storage and computational power. "Success will be judged on useful outputs, inputs and performance outcomes including around capacity, latency, and throughput. For those looking to charge based on usage, GPU hours and TPU hours consumed (a bit like electricity in an industrial power station) will be useful measures for charging entities. Whether on the supply or consumption side of AI and AI infrastructure, success will also be judged on speed to market whilst also delivering demonstrable governance and on the ability to comply across multiple legal and regulatory regimes," says Walker-Osborn.

The US – policy tailwinds, trade tools and export controls

The United States is at a watershed moment for AI infrastructure investment. Momentum is driven by federal initiatives and growing private sector activity. From its earliest days, the second Trump administration has prioritised significant new investment in AI infrastructure, with landmark announcements being rolled out regularly.

On the first full day in office, 21 January 2025, the administration announced Project Stargate, a US$500 billion joint venture between OpenAI, Oracle, SoftBank and MGX, aimed at delivering up to 10 GW of domestic data centre capacity. In August, the administration agreed to acquire a 10 per cent equity stake in Intel to support domestic semiconductor manufacturing. It also made a deal with NVIDIA and AMD that allowed the companies to secure licences to export certain AI chips to China, previously restricted, in exchange for the US government receiving 15 per cent of the profits. "These deals show the Trump administration remains opportunistic in driving US AI growth, even in jurisdictions like China where exporting US-origin AI items has historically been highly circumscribed," says Renee Latour, a Clifford Chance Partner based in Washington DC.

Private sector investment is also accelerating. In April, NVIDIA announced it would produce AI supercomputers entirely in the United States for the first time. Recently, NVIDIA committed US$100 billion to OpenAI to deploy 10 GW of AI data centres. OpenAI agreed to acquire 10 per cent of AMD and deploy up to 6 GW of AMD GPUs across AI infrastructure.
The administration has encouraged foreign partners to invest in US AI infrastructure, including a US$1.4 trillion commitment from the UAE to support data centre development.

"Wherever your business or entity sits in this AI ecosystem, the opportunity is clear. With such potential to monetise this technological shift, we are seeing huge investment and work in this area."

Charlotte Walker-Osborn
Knowledge Director

Trade and tariffs

Whilst the Trump administration has taken steps to encourage investment in US AI compute as well as to export the US AI stack abroad, it has also employed various new trade instruments to protect US national security and reduce dependence on non-US competitors in key industrial sectors. These measures make doing business in this space quite complicated.

"Tariffs is one of the words that comes across our desks most frequently in the trade space," says Latour. The administration has been very active in this area, especially with tariffs on copper – up to 50 per cent – which became effective on 1 August 2025. Potential tariffs on semiconductors, including the necessary wafers and chips for AI compute, also pose a significant risk to data centre supply chains. Similar risks apply to polysilicon, robotics and industrial machinery. All of these tariffs and trade measures are either in progress or already on the table. "This uncertainty affects sourcing opportunities and strategies for servers and GPUs that are essential to AI infrastructure, both domestically and abroad. The key is flexibility in sourcing and supply chain management," she adds.

The impact of these tariffs is felt directly in procurement, as organisations must adapt their sourcing strategies to account for cost volatility and potential delays. It is essential to build flexibility into contracts and supply chains to mitigate these risks.

> "Tariffs is one of the words that comes across our desks most frequently in the trade space."

Renée Latour
Partner

Export controls – dynamic and granular

On the export control side, the environment is incredibly dynamic and challenging, with expansions continuing to heighten restrictions. These controls govern the export, re-export and in-country transfer (which includes changes in end use or end user) of items subject to US export jurisdiction – particularly relevant here, chips. The rules are complicated and change not only through straightforward regulations but also through other measures, such as via specific licensing arrangements and "Is Informed" letters, which are targeted restrictions.

In October, the U.S. Department of Commerce expanded the Entity List by introducing the new "Affiliates Rule", which is similar to the 50 per cent rule administered by the Office of Foreign Assets Control (OFAC) for sanctions. Entities that are 50 per cent or more owned, directly or indirectly, by one or more parties on the Entity List or the BIS Military End User (MEU) list are now subject to the same export restrictions as those specifically identified on the Entity List itself. From a compliance perspective, this is incredibly challenging, as it requires deeper due diligence into ownership chains and more rigorous screening against existing risks and lists before proceeding with investments.

The risks of potential violations are high. Organisations must not only screen against existing restrictions and risks but also delve further into the ownership chain and ensure all compliance requirements are met before proceeding with transactions. "The answer is more, better due diligence, staying abreast of the topics as they roll out and trying as best as possible to, if not stay ahead of the game, at least stay current," says Latour.

What companies should do

To deal with these risks, companies need to design for supply-chain resilience. Use multi-sourcing and modular configurations, keep limited buffer stock where feasible and stand-up real-time trade and export governance with updateable playbooks. In addition, they should focus on sequence transactions with trade counsel alongside M&A, foreign investment and antitrust workstreams.

“We are seeing the APAC region rapidly transforming into a prime destination for AI infrastructure investment.”

Clarice Yue
Counsel

The investment climate in APAC

Governments across the APAC region are actively encouraging the shift from traditional data centres to AI factories. “We are seeing the region rapidly transforming into a prime destination for AI infrastructure investment,” says Clarice Yue, a Clifford Chance Counsel based in Hong Kong. Many countries are promoting foreign investment – Singapore, for example, offers targeted incentives such as grants for energy-efficient infrastructure and AI development, alongside streamlined approval processes for foreign technology investors. In Hong Kong and Australia, regulatory sandboxes provide flexible environments for AI innovation, lowering entry barriers for new projects. Japan and South Korea are modernising infrastructure with investments in green energy and advanced cooling to meet AI’s high processing demands. On a regional level, frameworks such as the ASEAN Digital Master Plan are harmonising standards across APAC, putting the region at the forefront of the global AI infrastructure landscape.

Securing advanced hardware in APAC

GPUs and other semiconductor chips are the heart of AI data centres. “Export controls, trade restrictions and geopolitical tensions are putting pressure on the supply of advanced chips for AI infrastructure” says Yue. In response, APAC countries are implementing a mix of domestic investment, regional cooperation, supply chain diversification and contractual measures to address these risks. Several countries are prioritising domestic semiconductor manufacturing and supply chain diversification – Japan has invested heavily in revitalising its semiconductor industry, partnering with Taiwan Semiconductor Manufacturing Co Ltd (TSMC) to build new chip fabrication plants, for example, while India has launched the Semicon India initiative for chip manufacturing and design initiatives and investment. Data centre operators in Singapore and Australia are sourcing GPUs and other chips from multiple vendors, including both US and Asian suppliers, to avoid over-reliance on a single source. Governments are also strengthening regional cooperation, with South Korea announcing multi-billion dollar investments to secure the supply of advanced chips for AI and other critical technologies.

Contracts in APAC

Various contractual measures are being implemented to address supply chain risk. For example, data centre operators are building in specific protections from both the procurement and customer contract sides. “On the procurement side, contracts with suppliers often include export control clauses, multi-sourcing rights, buffer stock arrangements, and flexibility to substitute components if disruptions occur, addressing potential export restrictions or delays,” says Yue. On the customer side, operators incorporate service-level agreements with clear force majeure terms, limitation of liability clauses and provisions allowing for technology substitutions and timely client notifications in the event of supply issues. This dual contractual approach helps operators maintain operational resilience and client trust amidst global supply chain uncertainty.

Data and localisation in APAC

“The main regulatory challenge in APAC is the patchwork of national laws, with varying degrees of maturity and differing approaches to data protection and data sovereignty,” says Yue. Navigating the regulatory landscape for data centre operations is complex, as international data sets drive AI factories and data centres. There are stringent regulations in China, Indonesia and Vietnam regarding localisation and data sovereignty. Operators must build compliance into their operational models from the outset, designing to meet these data regulations and ensure operational scalability and competitiveness globally.

Europe and the UK: competition and foreign-investment controls

Antitrust – areas of focus

Antitrust authorities are engaged in a balancing act – they must encourage innovation and attract AI investment, especially in the UK and the EU, given the current geopolitical competition and tensions. Regulators are keen to avoid stifling innovation but are also determined to prevent the emergence of entrenched positions that they perceive to have been the case before in the digital space.

"When you listen to regulators speak about this space, one often gets the feeling that they expect or would like AI to have a corrective influence, injecting new powerful players into the market," says Stavroula Vryna, a Clifford Chance Partner based in London. "A key concern that companies should be prepared to address, is access to key inputs such as GPUs, compute infrastructure and proprietary data sets." Many regulators are concerned that if key inputs may concentrate in the hands of a few players, creating market power, that market power could be abused to foreclose rivals.

"This is playing out at the moment, with much attention on NVIDIA's large investment into OpenAI," Vryna says. Regulators are looking very closely at anything resembling exclusivity in AI partnerships, and anything that may appear to be discriminatory preferencing in terms of granting access, especially with respect to compute.

"A key concern that companies should be prepared to address, is access to key inputs such as GPUs, compute infrastructure and proprietary data sets."

Stavroula Vryna
Partner

Foreign investment screening in Europe and the UK

Foreign investment scrutiny is now a given for anyone investing in AI infrastructure in Europe or the UK. This covers the full spectrum of the AI stack, including data centres, compute facilities and GPU/semiconductor chip supply chains. In the EU, nearly every member state operates a national security screening regime, and, unlike merger control, there is no one-stop shop, so investors may face up to 25 parallel FDI reviews. "If you're investing in AI infrastructure in Europe or the UK, you should assume that's part of the deal, and that includes the gamut of the AI stack and data centres, compute facilities of other types, supply chains for GPUs, all of it," says Vryna. The EU foreign investment regulation has a cooperation mechanism, so when you file in one country, every other EU member state and the European Commission are notified, increasing awareness of investments across jurisdictions.

AI infrastructure is generally seen as critical technology, which means it will usually trigger a mandatory and suspensory FDI filing before a deal can close. Even minority investments, sometimes as low as 10 per cent or less, can trigger FDI reviews in certain EU Member States. "The thresholds for transactions to be notifiable for investment review, especially in the AI space, tend to be relatively low, so we don't necessarily always need an acquisition of control, like in merger control regimes. Even minority investments of 10 per cent or even less, in some cases, can trigger review which is something that parties should keep in mind," Vryna says.

The situation is very similar in the UK, where the regime is being updated to make it explicit that AI infrastructure and third-party data centres are covered, with mandatory reviews triggered by such investments in certain cases.

How businesses should deal with antitrust and foreign investment scrutiny

Given the complexity of the regulatory landscape, businesses need to be proactive and strategic in their approach. "Early engagement and an understanding of interconnected reviews are essential. You will have antitrust, merger control reviews, FDI reviews, and all those reviews need to be sequenced appropriately, and the sequencing sometimes is the difference between meeting a long stop date and worrying about missing it," says Vryna. Having a single, globally coordinated legal team is often the most effective approach. "A one-stop shop in terms of counsel support often helps very much – having a one global coordinating counsel looking after this whole set of reviews tends to have the best outcomes for clients in my experience," she adds.

Europe: sovereignty, AIGF and the "build-to-certify" approach

"AI infrastructure has become highly politicised in Europe, with control of compute now seen as strategic as energy was 20 years ago," says Patrice Navarro, a Clifford Chance Partner in the TechDigital Group. Compute sovereignty has become an EU and member-state priority. It influences where capacity is built, who controls it, and which workloads are eligible to use it.

The AIGF initiative

The AI Gigafactory initiative (AIGF) has been developed by the European Commission and a body called the UHPC. It is designed to position the EU at the forefront of global AI innovation. It proposes very large EU-controlled compute campuses, open under defined access conditions and targeting more than 100,000 advanced AI chips per site. Under the Commission/EuroHPC consultation, AI Gigafactories are envisaged as public–private partnerships coordinated by an EU-headquartered entity or an EU Member State.

The financing model is public-private partnership, with potential public funding of up to about 35% of eligible capital expenditure on a case-by-case basis. Public support may cover a share of eligible CAPEX, with OPEX largely borne by private partners.

From colocation to outcomes

The move from traditional data centres to AI factories marks a shift from selling space and power to selling outcomes with contracts increasingly pricing and measuring GPU hours, training throughput, inference latency and queueing or priority. Service levels need to reflect these performance realities and to manage multi-tenant contention. "AI factories are like restaurant kitchens, where data centres are the fridge and GPUs are the ovens, transforming data into AI services for clients," says Navarro. Early integration of sovereignty and regulatory layers is essential; compliance cannot be an afterthought. Everything must be organised to reach the required certification level, such as SecNumCloud or EUCS, and to comply with the AI Act, Data Act, GDPR and cybersecurity rules."

Sovereignty in practice

Even without a single legal definition of "AI sovereignty", market expectations are converging. Effective EU control should extend to administrative access, key management in certified HSMs, update paths and tamper-evident logging. For the EU, alignment with EU cybersecurity certification (including EUCS as it arrives) and, where relevant, SecNumCloud-style safeguards to strengthen trust with public-sector and regulated clients. "You have to prove compliance to regulators, and you have to reach a certain level of sovereignty in most cases. There are so many aspects to take into consideration regarding this. It's a question of aligning all these layers together – compliance with AI laws, data regulation, and cybersecurity laws and certification," says Navarro.

"AI infrastructure has become highly politicised in Europe, with control of compute now seen as strategic as energy was 20 years ago."

Patrice Navarro
Partner

Operator checklist

- Plan and structure up front, including for regulatory compliance, factoring in the changing international trade landscape in order to make design choices which maximise opportunity, ensure access to materials and skills and build for ongoing governance and auditability. Ensure audit trails to aid compliance
- Consider certification choices upfront
- Consider the pros and cons of establishing a sovereign control plane for your business model, if relevant (by way of example, in the EU with EU-resident keys and ring-fenced EU support at higher tiers, supported by clear administrative workflows)
- Utilise your contracts to allow for flexibility in the event of significant changes in the regulatory landscape and/or changes to trade, foreign investment laws and screening and tariffs that could significantly affect the business model
- Agree AI-grade service-level agreements that capture latency, through-put, queueing and red-team cadence
- Provide for exit and portability, with defined formats, timelines and resourcing

Regulatory alignment and what businesses should do

"Design for the AI Act where applicable, including documentation and transparency for general-purpose model providers and risk-management for designated models," says Navarro. Build exit and portability into the architecture in line with the Data Act, including the end of switching fees from January 2027. Implement organisational security and incident-reporting processes consistent with NIS2. Incorporate foreign investment screening and export-control constraints into site selection, ownership, contracting and support models at the outset. With regard to the finance and accounting structure consider IFRS consolidation early. "Governance rights that amount to control can bring an asset on balance sheet for a private or public partner, which affects financing terms, covenants and the allocation of risk and reward," he says.

Across regions, the common thread is "structure first, operate second". AI factories that are designed from day one for sovereignty, compliance and useful capacity will attract workloads, approvals and finance. Those that are not may face delays, stranded capacity and under-utilised assets.

What next?

The potential for net gain for business and society from the AI wave is clear. This summary merely scratches the surface of some of the key regulatory areas to think about within parts of the world (before we even layer on regulatory considerations for businesses building AI focused data centre infrastructure in space). Additionally, areas such as financing, routes to market, energy considerations, maximising intellectual property and business value, potential for M&A activity to grow market share and/or ensure skill sets are available to build and/or leverage AI and AI infrastructure are crucial to weigh up and factor in. Critically, some of the regulatory, trade and other impacts mean that sometimes a net win for your business in one country may mean a net loss for your business in another as you weigh up the incentives to pivot your business in certain directions.

In order to maximise the ability for your business to derive the benefits, it is important to engage with all of these areas as early as possible, taking both a detailed and a helicopter view before building a plan that will work to achieve your organisational ambitions.

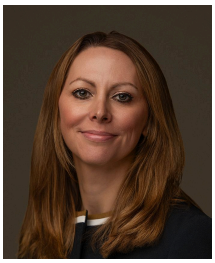
Contacts

Renee Latour
Partner, Washington

+1 202 912 5509
renee.latour@cliffordchance.com

Patrice Navarro
Partner, Paris

+33 1 4405 5371
patrice.navarro@cliffordchance.com



Charlotte Walker-Osborn
Knowledge Director –
Tech Group (UK Lead), London

+44 207 006 2662
charlotte.walker-osborn@cliffordchance.com

Stavroula Vryna
Partner, London

+44 207 006 4106
stavroula.vryna@cliffordchance.com

Clarice Yue
Counsel, Hong Kong

+85 2282 58956
clarice.yue@cliffordchance.com

Clifford Chance

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.