HERBERT SMITH FREEHILLS

DATA CENTRES

GLOBAL PERSPECTIVE ON KEY ISSUES

JULY 2024

Growing data centre demand

Demand for data centres continues to grow globally, driven by the increased computing requirements for generative AI and machine learning and continued demand for data and connectivity, cloud computing, the deployment of 5G networks and IOT capability.

> Some estimates suggest current data centre assets in Europe will need to more than double over the next few years to keep up with growing demand

Around the world, data centre demand is outstripping supply – some estimates suggest current data centre assets in Europe will need to more than double over the next few years to keep up with growing demand, Europe is currently lagging the US on capacity and is now racing to close the gap while also experiencing double-digit growth rates, and Africa and APAC are both seeing unprecedented levels of demand.

Development pipelines are widely viewed as insufficient to meet the increased demand over the coming years.

Significant capital will be needed to expand existing facilities and build out greenfield developments.

JVs between financial investors and developer/owner operators are now becoming increasingly prevalent in order to provide such funding. Investors are also looking to capitalise on the significant energy requirements of data centres through investing in renewable energy assets, eg wind and solar, as well as storage, green hydrogen and carbon credit projects.

Investment opportunities

The global surge in demand has attracted the attention of investors of all types – growth capital, buyout, real estate and, increasingly, infrastructure investors – given the long-term, inflation-linked cash flows and risk-adjusted yields on offer.

Investment in data centres has more than doubled in recent years – despite recent economic headwinds – and, as inflation falls and interest rates stabilise, we expect data centre investment to grow exponentially. The sector is also becoming increasingly nuanced, as investors carve out differentiated strategies based on their own preferences and capabilities. Those players who are investing thoughtfully along the data centre value chain, where they can add most value, and who can create unique capital solutions that scale to meet the capex required to put the infrastructure to work, will succeed here.

Investing in data centres is not without its challenges, however, and we are seeing:

- ***Development challenges:*** Increasingly difficulty in building new data centres in some jurisdictions – due in some cases to practical factors (such as the lack of suitable land in densely-populated urban areas and lack of power supply or grid connectivity), and in some cases to legal or planning factors (such as Singapore's 4-year moratorium on new builds).

  Other markets, however, are actively trying to attract data centre investment, and certain secondary markets, with available land for development hubs and robust power supplies, stand to attract more data centre operators.

- ***Construction and design risks:*** Increasing costs of construction, data centre equipment, and labour rates, and less predictable development timelines, are making it difficult for developers to commit to deliver projects to fixed timelines and budgets, and are requiring increased flexibility to be built into construction and supply contracts.

- ***Power constraints:*** Data centres currently consume around 2-3% of global electricity usage – this is forecast to grow significantly.

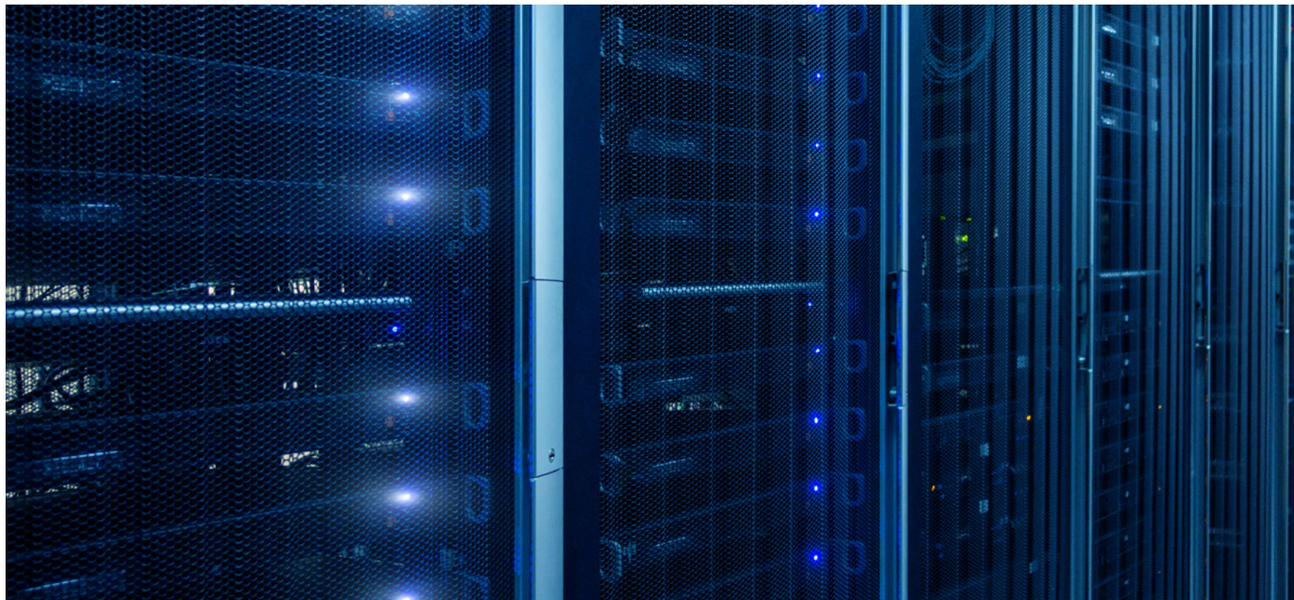
  Power availability and reliability is becoming an increasingly import factor in evaluating development opportunities. Many countries have adopted restrictions on adding major new loads to the grid, and some (such as the Netherlands and Ireland) have issued a 'pause' on new developments in an effort to reduce the strain on power grids.

  The transition towards net zero is also driving innovation in energy solutions for data centres and generating hybrid investment opportunities – with opportunities for co-located solar or wind assets, or investment in lithium-ion or other battery technologies.

- ***Increased regulatory regimes:*** The rapid growth in data centre demand has been matched by a similarly rapid growth in the regulatory regimes impacting investing into, and the operation of, data centres.

  Several FDI regimes have classified the processing and storage of data (particularly governmental or sensitive personal data) as being 'critical infrastructure', and this will likely continue as a trend.

  Operators are seeing increasing regulation across several fronts – from an energy perspective (eg the EU's Energy Efficiency Directive reporting requirements), in relation to the protection of personal data and privacy, and the introduction of licensing regimes.



Selection of key legal issues

> Given the challenges that lie ahead for operators, developers and investors, we have brought together our global specialists for their view on key legal issues

Given the challenges that lie ahead for operators, developers and investors, we have brought together our global specialists for their view on key legal issues – covering the full life-cycle of data centre development and operation, from securing appropriate land and necessary consents, through to construction and access to power, trends in key customer and supply contracts, managing ESG and regulatory regimes, as well as financing and M&A activity.

We are pleased to be able to share with you some insights about the key legal issues we are seeing around the world, and some reflections on navigating data centre investment opportunities.

Location, location, location

Key to the development of new data centres is securing land in suitable locations, along with the requisite rights over such land (and surrounding land, as necessary) – including the right to develop and operate the data centre and critical supporting infrastructure.

Suitable land and supporting infrastructure

Until more recently, the conventional hubs for data centres have been major cities – leveraging the advantages of robust telecom connectivity and target client demographics.

However, there is a developing trend of exploring opportunities outside of these traditional hubs, with a focus on smaller cities where land is usually more available and cheaper, power constraints can be less of an issue, and the requisite permits can be easier to obtain. For example in Europe, the developing trend is to focus outside of the FLAP-D markets (Frankfurt, London, Amsterdam, Paris, Dublin).

For some regional or 'edge' plays, securing access to relevant expertise and specialists (eg suitably experienced engineers) can prove challenging, which may provide those operators with access to local expertise with a competitive advantage.

Consenting

Successfully navigating the relevant consenting processes for data centres often involves a delicate balancing of interests in what can be a highly political climate.

In support of new development applications, we have seen operators successfully rely on demonstrating the benefits of 'agglomeration effects' which can result from data centre developments, including:

- decreased latencies for nearby service users, leading to multiple service users relocating near to them; and
- positive socio-economic impacts resulting from the data centre project.

> Consenting authorities are increasingly focussed on sustainability, and any sustainability synergies resulting from a new development can prove to be significant in the consenting process

Consenting authorities are increasingly focussed on sustainability, and any sustainability synergies resulting from a new development can prove to be significant in the consenting process – for example, connecting the data centre to local district heating networks in order to deliver waste heat as a heating source for surrounding communities.

Demonstrating a developer's sustainability credentials is an increasingly important aspect of consenting processes around the world, as well as evidencing that a proposed data centre can be delivered and operated within a defined sustainability envelope.

Building your data centre

Due to a number of key factors – evolving technology, heightened reliability requirements, supply chain risks, and costing and inflationary pressures – ensuring upfront consideration of the following issues will be critical to the successful delivery of data centre projects.

Procurement structures

Fixed-price, lump sum Engineering, Procurement and Construction (or EPC) Contracting by-and-far remains the preferred approach for data centre developers, due to the complete wrapping of quality, time and cost risk under such an arrangement.

However, EPC models are increasingly coming under strain due to global cost and supply chain pressures. These pressures have resulted in other contracting models – such as direct owner procurement (with corresponding free-issuing); construct-only; EPCM; ECI-style models; Managing Contractor models; and Integrated Owners Team – being canvassed as options for the delivery of project developments.

Each of these models have their pros and cons, and adopting the best contracting structure will, ultimately, depend on the developer's risk appetite and preferred pricing methodology.

Cost and supply chain risk

Recent trends in contractor and supply markets have seen the management of cost and supply chain as considerable risks in the successful delivery of data centres (eg cost pressures from recent steel prices increases).

While an up-front and realistic assessment of the likely costs of developing a data centre, and the likely supply chain limitations will be the most effective way to manage this risk, the following will also be useful mitigation tools:

- appropriate contractual levers;
- factoring in additional program buffer/float;
- ensuring reporting is providing a realistic picture of project development; and
- ensuring an adequately resourced owner's team is properly managing and monitoring contractors and suppliers.

Interface risk

> The delivery of complex and large-scale data centre projects on time, on budget, and to required standards of performance is not always straightforward and, not surprisingly, such projects can give rise to disputes

The delivery of complex and large-scale data centre projects on time, on budget, and to required standards of performance is not always straightforward and, not surprisingly, such projects can give rise to disputes, particularly over delays (and liquidated damages), especially when there are multiple parties and subcontractors involved.

Managing the interface risk between different systems and contractors is fundamental to the successful delivery and operation of a data centre (particularly once the data centre goes live) – not only contractual arrangements, but also through promoting a collaborative culture.

Carrot and stick – incentivising performance

Developers need to ensure that their development contracts include adequate 'carrots and sticks' to incentivise performance.

Performance guarantees (linked to performance liquidated damages) and compensation for delays (often in the form of delay liquidated damages) are regularly included in the contracting arrangements for data centre project development.

Operation and maintenance

Data centre utilisation will likely ramp up and down over time across its full nameplate capacity.

Accordingly, data centres must be designed to allow for all systems to operate across these operating fluctuations (without needing all systems to operate at full nameplate capacity at all times).

Allowing for such flexibility in design and operation will, of course, have significant impacts on the cost base and profitability for a data centre.

Given that 'downtime' in a data centre must be carefully controlled and managed, developers should factor in the ready procurement of spare parts early in their project planning. Establishing arrangements for spare parts in key equipment supply contracts is far more efficient than needing to shut down part of a data centre due to a long lead time on spare or replacement parts.

Insurance

It is critical for the project sponsors to ensure that sufficient insurance coverage (across the entirety of the project) is maintained throughout the full life cycle of a data centre development.

In some cases, developers may consider procuring an 'owner-controlled' insurance programme for the entirety of the data centre development, to simplify the insurance arrangements and insurance costs (with multiple sub-contractors) across the project.

Key customer and supply side contracts

Revenue for data centre operators is derived from long-term contracts with customers. Depending on the business model, these may be hyperscalers or wholesale or retail colocation customers (typically large enterprise and government customers).

Certainty of those contracted revenue streams is critical for data centre operators and investors alike. Key considerations include:

- contract term and extension rights, and whether customers can decrease the occupied space with attendant decreases in revenue;
- any early termination rights for customers;
- to what extent the operator can increase the applicable charges over time (eg by CPI).

Delays

Large customers typically require some commitment around the date by which service will commence, so, in terms of assessing the risks around potential delays, consideration should be given to:

- whether the operator may be liable for liquidated damages for delays (or, in some cases, risk of termination and exit in case of severely protracted delays);
- to what extent such exposure has been passed through to the construction partner for construction related delays.

In some cases, large customers may also require flexibility to delay service commencement post completion of the relevant construction and commissioning work (eg to allow the customer to schedule their own server fit-out work in line with other network optimisation priorities).

Customer rights over additional space

> The ability to commercialise existing and future data centre space will be a key feature of an operator's growth strategy

The ability to commercialise existing and future data centre space will be a key feature of an operator's growth strategy, and such ability needs to be assessed considering any rights granted by the operator to existing customers who may require 'reservations, 'options', or other pre-emptive rights over additional space that is, or may become, available.

This can involve an assessment of:

- the scope and duration of such reservations, and whether such rights are only paid for if exercised, or if there is a price associated with the grant of the reservation;
- the extent to which those rights may limit the operator's ability to commercialise additional capacity in the future.

Supply-side exposures

In addition to power, other material operating costs for data centre operators include the cost of operating and maintaining networking equipment and HVAC systems; staffing costs; and security costs.

Depending on the operator's service delivery model, some of those aspects may be managed in-house and others may be outsourced to third party suppliers.

Understanding the relationship between the key supply-side cost profile and the customer-side revenue profile can be particularly helpful in modelling the reliability of a data centre's operating margin. Key considerations include:

- whether supply-side costs are fixed, or whether the supplier can increase pricing (and, if so, on what basis, and whether this is subject to specified caps/limits);
- whether supply-chain cost increases (eg power or emissions levies) can be passed onto customers (and, similarly, whether any such pass-through is subject to specified caps/limits).

Telecommunications

Depending on the jurisdiction and scope of services offered, aspects of the data centre services offered by the operator could be, or include, regulated activities. For example, offering connectivity in the form of IXPs (Internet eXchange Point); network endpoints from telecommunications carriers; metro fibre and cable networks; or rooftop licences for transmitter equipment, may be regulated.

Several regulatory regimes (for example, Thailand, China and Singapore) now require data centre operators to obtain permits or telecommunications licenses, particularly if the relevant data centre offers connectivity solutions that may amount to the facilitation of telecommunications services.

Where relevant, consideration should be given to the appropriate allocation of risk and backing this off against the relevant telecommunications supply contracts.

If the data centre operator's business model extends beyond providing physical infrastructure, then consideration should also be given to whether other regulatory and compliance obligations may be triggered, such as (for example) compliance with data protection laws or interception laws (see the *Privacy, Cyber Security and National Security* section).

Powering your data centre

Energy design, procurement and cost are significant issues for a data centre. The cost of power is easily the single largest component of a data centre's operating costs.

Energy efficiency

As energy efficiency is a key factor in the profitability of a data centre, energy efficiency is a key focus in the design, construction and operation of data centres.

Data centres regularly include specific energy efficiency metrics to monitor, post-completion, the energy efficiency (the 'PUE') of a data centre. This can, of course, be linked to service levels and service credit regimes, and, in some cases, remediation and exit rights.

The revised Energy Efficiency Directive, published in September 2023, introduces an obligation for EU Member States to monitor the energy performance of data centres, and states that an EU-level database will collect and publish information relating to the energy performance and water footprint of data centres.

Energy supply

There are various options when it comes to powering a data centre, with the options mostly coming down to location of the data centre and the relevant jurisdiction.

In some jurisdictions, financial energy hedging arrangements can be used to help manage exposure to energy market volatility.

Connecting to the grid

In some jurisdictions, data centres can "plug into the grid" and take power from the market at a wholesale level (sometimes known as a 'market participant').

However, in many countries there are now restrictions on adding major new loads to the grid. Permission to build or expand is becoming more difficult to obtain, prompting questions over where data centre clusters are located. Achieving more, with the same amount of energy or less, will be a recurrent theme throughout the year ahead that will continue into the foreseeable future.

Where the market does not allow for this, or the data centre's requirements are not as large, we regularly see data centre operators entering into energy supply agreements, or power purchase agreements (known as PPAs), with energy retailers.

Remote data centres

In remote locations, data centres may be powered by an independent power producer (known as an IPP) or produce power through an 'islanded' system.

Where an operator creates their own islanded system, third parties may also seek to procure energy from that system (which can provide additional revenue streams and help with the efficiencies of a remote data centre).

Renewables

A key trend in the sector is the movement towards pairing data centres with renewable energy assets – such as solar and wind.

In considering the implementation of renewable energy assets as part of a data centre's energy solution, investors/operators will need to assess whether the renewable energy generation asset is:

- on the same site, or co-located, with the data centre; or
- a grid-connected asset, supplying electricity to the data centre via a PPA.

Continuity is king

Continuity of power for a data centre is essential.

Outages can mean costly financial consequences and reputational damage for data centre operators – causing business interruption for customers, triggering liability for service credits, reductions in service fees and potentially other rights (including, if severe enough, the termination of customer contracts).

In addition to more traditional technologies which continue to be used as part of a data centre's power continuity arrangements (such as rotary/motor generation, eg DRUPS), lithium-ion batteries are also starting to come into use (as are newer battery technologies, such as vanadium batteries). As these solutions continue to become cheaper and more readily available, we anticipate batteries becoming much more common features in data centres.

Customer considerations

Energy supply arrangements are a key discussion point between data centre operators and customers (particularly large colocation customers).

Such discussion may often include:

- if the customer will utilise power supplied under the operator's power supply arrangements, or will enter its own direct arrangements for power with a supplier;
- the basis of charging – namely if the operator charges for power on a pass-through basis or if power costs are wrapped into the operators pricing (and any adjustment mechanisms for cost increases);
- if the operator passes through the cost of all power used at the data centre facility to customers, or only the IT power component; and
- the operator's liability for power supply failures (such as non-availability due to power issues).

Financing your investment

Debt finance of the acquisition and development of data centres is at a relatively early stage and the model used may vary depending on the characteristics of a specific financing.

The principles applied are often based on project financing – though a structure more akin to a real estate financing, leveraged financing or a broader Holdco or corporate debt financing (or some combination of these models) might also be used instead, depending on the view that lenders take to a specific data centre project.

This hybrid approach is not unique to data centres and is regularly used in financing other types of digital infrastructure, where concepts that typically arise in the context of real estate finance or traditional infrastructure finance (such as planning concerns) sit alongside payment flows under contracts which might be more typically seen in project, or even leveraged, finance.

Key focus areas for lenders

Typically, the key 'data centre-specific' focus areas for lenders will fall into the following categories:

- **site:** as well as the usual real estate, planning and construction-related concerns, access to power and water supplies will be key (as well as the associated assets available, such as a source of renewable energy or a battery energy storage system);
- **revenue flows for debt servicing:** the make-up of the relevant customer base will clearly be of interest to lenders, and the terms of the relevant customer contracts will need to be bankable;
- **colocation customer equipment:** understanding the division between operator equipment and colocation customer equipment that is housed in the data centre will be of interest to lenders as regards the scope of their security package;
- **customer termination rights:** the commercial sophistication and leverage of major customers such as hyper-scalers may also give rise to concerns around termination rights in customer contracts. Conversely, customers may be prepared to enter into direct subordination, non-disclosure and attornment agreements with lenders, under which the customer agrees not to terminate their contract without giving lenders prior notice and a remedy period, in return for the financiers agreeing not to disturb the customer's use of the data centre.

Financing options

The most appropriate financing option can vary, depending on the acquiror and the exact nature of the asset being financed – for example:

- funding using the capex lines in general corporate debt facilities might be an option for some corporate borrowers;
- where a portfolio of assets is being financed, the available options will be increased by cross-collateralisation. Options will also depend on what stage those data centres have reached; for example, if a combination of greenfield and brownfield (sometimes called "yellowfield") assets are being financed, the revenue generated by some assets could be used to service the overall financing of the other assets in development;
- for a portfolio of operating data centres, a Holdco financing may be the most appropriate;
- in some cases, a green bond may be an option, where the data centres to be financed satisfy the relevant criteria;
- in the case of centres using a DCaaS model, trade receivables financing may provide access to a broader investor base.

> Where a portfolio of assets is being financed, the available options will be increased by cross-collateralisation

Sustainability considerations

Sustainable finance may be integral to data centre financings, as in a green bond, or a green or sustainability-linked loan facility. Alternatively, ESG issues (see the *ESG and data centres* section for further discussion) may arise in the context of regulatory requirements, with requirements for disclosures to be made to the lenders and publicly, and requirements for compliance with environmental law.

ESG and data centres

ESG risks, compliance and reporting are at the forefront of data centre sponsors' and investors' corporate agendas.

Managing ESG related risks in connection with data centre projects, including internal initiatives and public commitments, can help unlock business value and protect future resilience.

Supply chain risk identification

Managing business critical ESG impacts requires a continuous improvement approach to supply chain risk identification and management – ensuring robust compliance and governance processes are in place in order to:

- identify risks, and to ensure that compliance and diligence supports securing capital and credibility in the market;
- raise debt that satisfies relevant environmental policies and investors' ESG mandates;
- manage supply chain and operational risks, including environmental and social impact;
- decarbonise operations and supply chains;
- respond to ESG-related allegations, claims, investigations and activism.

Disclosure and reporting

The growing burden of ESG reporting, and the readiness of regulators, investors and other stakeholders to scrutinise disclosures – whether voluntary or mandatory – calls for a sophisticated and coherent approach by data centre sponsors and investors. Reporting expectations and greenwashing is a global focus for activists and regulators alike, with disclosure expectations only likely to increase.

The introduction of global climate and sustainability reporting requires data centre sponsors and investors to determine the applicable reporting frameworks and the disclosure of significantly more robust climate and sustainability related risks, opportunities, targets and metrics.

Greenwashing

> There have been significant recent developments (including government inquiries) in relation to misleading and deceptive conduct in 'green' and 'social' claims

There have been significant recent developments (including government inquiries) in relation to misleading and deceptive conduct in 'green' and 'social' claims. We expect that regulators, and regulatory enforcement in general, will become an increasingly important focus in this space. Climate plans and carbon commitments are likely to be a key risk area for greenwashing allegations.

Data centre sponsors and investors should remain aware and responsive to potential risks from making misleading claims about environmental and sustainability commitments. It must be made clear when climate targets will be met through methods other than reducing emissions from supply chains – such as by investing in tree farms, or other types of carbon offset.

Data centre sponsors and investors should also consider whether their services enable greenwashing by other companies.

Business and human rights

The business and human rights landscape is evolving rapidly.

Since the unanimous endorsement of the United Nations Guiding Principles on Business and Human Rights in 2011, there has been a steady convergence of regulations and standards in this area towards a consensus that business enterprises must take active steps to ensure respect for human rights and to avoid causing or contributing to adverse human rights impacts. This includes undertaking human rights due diligence to identify and avoid risks to human rights in business operations and supply chains.

'Soft laws' have increasingly hard consequences as they become part of national legislation (for example through the United Kingdom and Australian modern slavery legislation) and are increasingly reflected in commercial and financial arrangements.

We help our clients to identify and respond to the adverse impact human rights' risks have on their business and supply chains and advising on the application of relevant domestic and international laws and standards. This includes the development of human rights policies, human rights due diligence, and impact assessment, crisis response and dispute resolution.

Privacy, cyber security and national security

The consequences of cyber-attacks are soaring – along with their scale, frequency and sophistication.

Data centres are a prime concern given the volume and value of data involved and the interconnectedness with other critical systems.

Increasingly, data centres are also coming under scrutiny from intelligence agencies and other government bodies, due to the risk they present from a national security and critical infrastructure resilience perspective.

Privacy and cyber security

The effects of privacy and cyber incidents at data centres can flow down to other vital infrastructure such as hospitals, airports and utilities – leading to operational shutdowns, undermining consumer confidence and causing real harm through identity theft and financial loss.

Compounding matters, 'bad actors' are continually adapting and looking to leverage new capabilities such as generative AI.

Data centres need to walk a fine line to ensure facilities, equipment and data are properly protected, and to assure customers in this regard, while also ensuring that responsibilities and liability are fairly allocated when an incident occurs. This can involve careful drafting of contractual arrangements with customers and vendors, with key issues often arising in relation to data breach incident response, audit rights, security measures and liability.

Data centre security and resilience

Many data centres form part of critical national infrastructure. They are often critical to telecommunications networks, cloud computing and e-commerce, as well as servicing key sectors such as banking, energy, aviation, utilities and manufacturing.

Data centres are of particular interest to nation-state sponsored (ATP) threat groups whose goals may include political and commercial espionage, as opposed to direct criminal profit – which has increased the level of interest from national governments and security agencies.

When a crisis occurs, lawyers are increasingly involved in coordinating critical activities such as engaging with the board, government, regulators and insurers, assessing operational impacts, reviewing compromised data, ensuring regulatory and contractual compliance, overseeing communications and executing a cyber extortion response strategy. Failure to appropriately manage these workstreams can have significant legal and regulatory ramifications.

Critical infrastructure reform

> Amongst an increasingly complex cybersecurity regulatory ecosystem, critical infrastructure reform has been a key area of change globally

Amongst an increasingly complex cybersecurity regulatory ecosystem, critical infrastructure reform has been a key area of change globally.

Critical data storage and processing assets, including data centres, are already attracting enhanced security obligations in some jurisdictions.

Many jurisdictions have also introduced legislation to enable intelligence agencies or other government bodies to intervene, audit, and secure data centres in the interests of national security, including by exercising powers to enforce ownership or governance requirements, or directing that customers meeting certain criteria are prohibited from using the data centre (effectively precluding operators of data centres from providing services to certain sectors).

National security concerns can be particularly heightened when there are concerns that ownership structures could lead to foreign nation states being able to exert undue interest or control over data centre operations.

Wiretapping/interception

Another manifestation of this risk for data centre owners and operators is that the volume of data flowing through data centres means they are on the receiving end of requests from intelligence agencies to permit interception of data in transit or extraction of data held on servers (sometimes under Court orders issued to facilitate interception for national security or other reasons).

Buying and selling data centres

We have deep experience and expertise advising clients on corporate transactions for data centres, including investors acquiring minority and majority stakes in data centre businesses, and advising investors establishing joint ventures to target hyperscale customers.

FDI regimes

The growing criticality of data centres to both governments and citizens is likely to result in FDI authorities increasing their focus on investments in data centres by foreign investors, as well as on issues such as data localisation and accessibility.

In several FDI regimes (eg Australia, the UK, the US and many EU member-states) the processing and storage of data (particularly governmental or sensitive personal data) is deemed to be critical infrastructure, meaning that a potential investor is required in many cases to obtain mandatory pre-completion clearance from the relevant FDI agency. Significant sanctions can be imposed for any failure to file.

FDI agencies also have the power to impose commitments as a condition for clearance, ranging from data/infrastructure access and security commitments to, in a worst-case scenario, prohibiting a transaction or ordering a divestment.

FDI regimes are continuing to evolve rapidly, merger control regimes also need to be considered: in some cases, a filing will be required even if there is no overlap in activities with the investor.

Development risk

Given investments are often made in data centre platforms which include greenfield sites, careful consideration should be given to whether, and to what extent, investors will assume development risk – see our earlier section on *Building your data centre*.

Ownership structure/funding

Joint ventures are often structured as LLPs, with equity interests determined by the value of the operator's contributions in the form of data centre assets and offtake agreements, as well as certain development rights, and the cash contribution of the institutional investor.

Secured credit facilities are typically obtained for part of the consideration paid to the operator for the sale, for development and construction costs, and for general working capital purposes.

Other important issues relating to structure and funding include how the capital needs of the JV group is drawn down, leverage policies, pre-emptive rights, and distribution policies.

Control rights

Minority/JV investors will wish to include a governance regime that requires their consent to be obtained with respect to various matters, corresponding to their ownership interest. In the context of data centre joint ventures, a matter which is particularly important is material amendment or termination of any customer contract – the threshold for consent is often set by reference to a certain net operating income of the business, development yield, total contract value or expected levered IRR to company (where the contract relates to a project).

Other important issues relating to governance include investor board representation, quorum and timing of board meetings, setting annual budget and business plans, and investor information rights.

Exit

> Investors, particularly those investing from close-ended funds, will need to ensure there are appropriate avenues to achieve liquidity

Investors, particularly those investing from close-ended funds, will need to ensure there are appropriate avenues to achieve liquidity. Typically, after a lock-up period, a minimum percentage of shareholders are entitled to initiate an IPO, recapitalisation, or combination of the group with another business (provided a minimum percentage IRR is met). This right is usually subject to reserved matters and a ROFO.

Income tax

In several jurisdictions, trusts, limited partnerships and other "tax transparent" vehicles are used to limit the imposition of local income tax on asset holding vehicles. Investors can use blocked or unblocked upstream structures to manage their exposure to tax/filing obligations in the jurisdiction in which the assets are held, and to optimise claims for foreign tax credits.

Where substantial foreign investors are involved in the ownership structure of a data centre operator, consideration should be given to managing the withholding tax on income distributions, as well as the tax that may apply on exit.

Consideration should also be given to the appropriate structuring of debt (including investor debt) having regard to the limitations in thin capitalisation and other rules relating to debt deductions.

Transactional taxes

Transactional taxes (such as stamp duties) apply in several jurisdictions around the world.

We are seeing a move to land-based taxes in many jurisdictions extending to freehold interests in land as well as fixed items.

For data centres, this will often mean that the land and infrastructure are dutiable on acquisition – but there can be exceptions to this for certain transactions/jurisdictions.

For indirect investors (such as through a fund), there can be an advantage in investing through a fund that qualifies for stamp duty concessions. Several jurisdictions have introduced such concessions for wholesale or retail funds.

Global specialists

Corporate

Emma Stones
Partner, London
Corporate
M +44 7562 438237
emma.stones@hsf.com

Gavin Williams
Partner, London
Corporate
M +44 20 7466 2153
gavin.williams@hsf.com

Mathias Dantin
Partner, Paris
Corporate
M +33 6 30 59 36 98
mathias.dantin@hsf.com

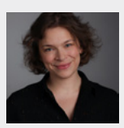
Tom O'Neill
Partner, London
Corporate
M +44 7827 303944
tom.oneill@hsf.com

Edouard Thomas
Partner, Paris
Corporate
M +33 6 09 02 78 20
edouard.thomas@hsf.com

Alberto Frasquet
Regional Head of Corporate EMEA
M +34 91 423 4021
alberto.frasquet@hsf.com

Guillermo Uriarte
Partner, Madrid
Corporate
M +34 91 423 4042
guillermo.uriarte@hsf.com

Energy



Sarah Pollock
Partner, London
Projects, Energy & Infra
M +44 7809 200522
sarah.pollock@hsf.com

Finance

Heather Culshaw
Partner, London
Finance
M +44 7809 200551
heather.culshaw@hsf.com

Armando García-Mendoza
Partner, Head of Finance, Madrid
Finance
M +34 91 423 4024
armando.garcia-mendoza@hsf.com

Technology, Media & Telecommunications

David Coulling
Partner, London
TMT
M +44 7809 200144
david.coulling@hsf.com

Dominic Rowe
Of Counsel, London
TMT
M +44 7395 375061
dominic.rowe@hsf.com

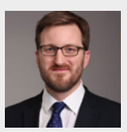
ESG

Silke Goldberg
Partner, London
ESG
T +44 20 7466 2612
silke.goldberg@hsf.com

Projects

Thomas Herman
Of Counsel, Paris
Projects, Energy & Infra
M +33 6 85 48 69 10
thomas.herman@hsf.com

Construction



Tim Healey
Partner, London
Projects, Energy & Infra
M +44 7809 200 034
tim.healey@hsf.com

Real Estate

Jeremy Walden
Managing Partner, London
Real Estate
M +44 7771 917952
jeremy.walden@hsf.com

Tomás Diaz
Partner, Madrid
M +34 91 423 4095
tomas.diaz@hsf.com

Anne Petitjean
Partner, Paris
M +33 1 53 57 13 55
anne.petitjean@hsf.com

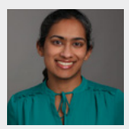
Martyn Jarvis
Senior Associate, London
Real Estate
M +44 7809 200572
martyn.jarvis@hsf.com

Disputes

Andrew Moir
Partner, London
Disputes & Cyber
M +44 7809 200434
andrew.moir@hsf.com

Competition, Regulation & Trade

Veronica Roberts
Partner, London
Competition, Regulation & Trade
M +44 20 7466 2009
veronica.roberts@hsf.com



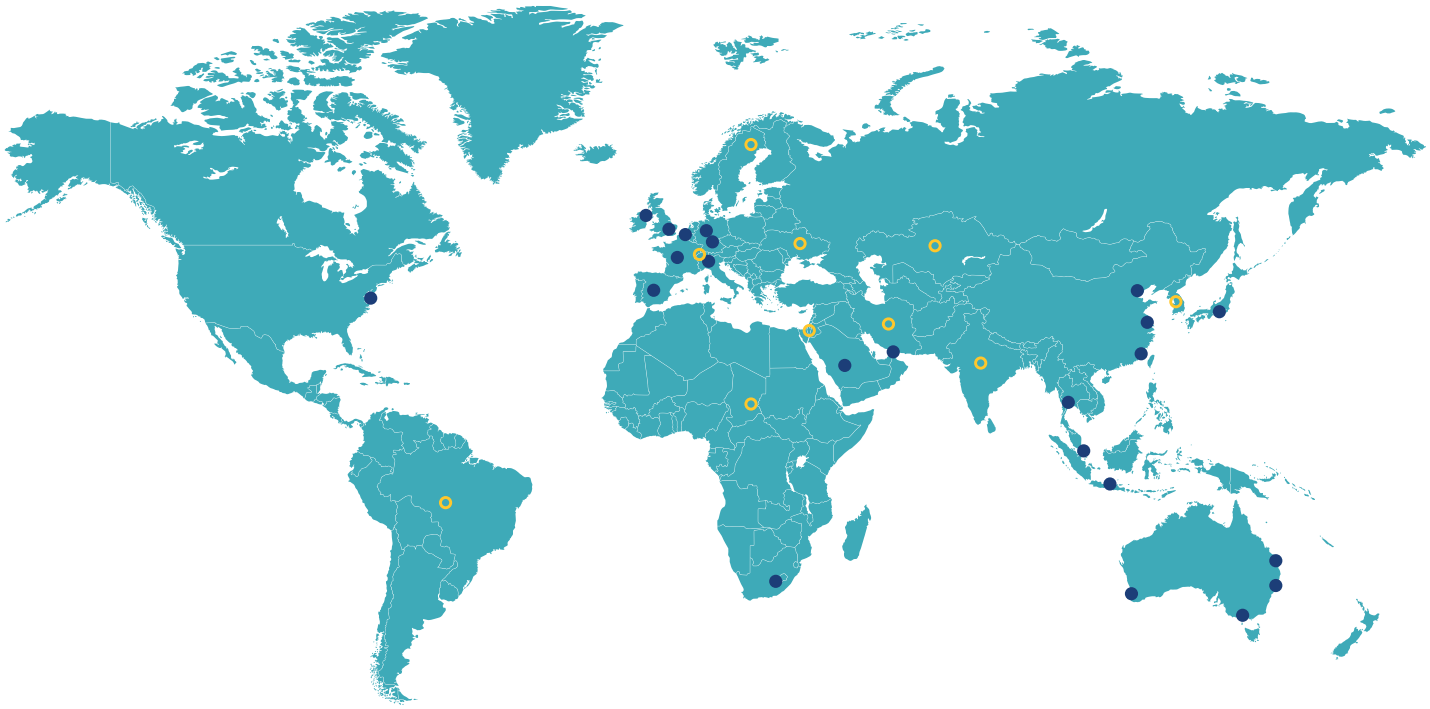
Natalia Rodriguez
Partner, London
Competition, Regulation & Trade
M +44 20 7466 7486
natalia.rodriguez@hsf.com

Public Law

Iria Calviño
Partner, Madrid
Public Law
M +34 91 423 4022
iria.calvino@hsf.com

Our global platform

As one of the world's leading law firms, we advise many of the largest and most ambitious organisations across all major regions of the globe. With over 5,000 people, including over 2,600 lawyers operating from our global network of 24 offices across Asia Pacific, Europe, the Middle East, North America and Africa, Herbert Smith Freehills is at the heart of the new global business landscape providing premium quality, full-service legal advice.



OFFICES

BANGKOK
BEIJING
BELFAST
BRISBANE
BRUSSELS
DUBAI
DÜSSELDORF
FRANKFURT
HONG KONG
JAKARTA*
JOHANNESBURG
LONDON
MADRID
MELBOURNE
MILAN
NEW YORK
PARIS
PERTH
RIYADH
SHANGHAI
SINGAPORE
SYDNEY
TOKYO

GROUPS

AFRICA
INDIA
IRAN
ISRAEL
KAZAKHSTAN
KOREA
LATIN AMERICA
NORDIC
SWITZERLAND
UKRAINE

* Associated office

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**