Data Centers

2025

Hogan Lovells

Contents

Introduction.

The data center industry is expanding substantially, largely fuelled by the rising demand for cloud computing services, big data analysis, and digital transformation efforts across various industries.

As organizations increasingly depend on digital infrastructure, it becomes crucial for project developers and investment funds to grasp the trends, challenges, and opportunities present in this sector.

For project developers and funds engaged in this domain, important factors to consider are choosing suitable locations based on criteria like connectivity and power supply, ensuring adherence to local laws, managing risks linked to investments in technology infrastructure, and seeking partnerships that can boost operational efficiency.

At their current stage of development, data centers are recognized as high-growth projects due to demands from AI and other computing needs while energy transition efforts are gaining momentum due to government incentives and regulations.

The data center market

During the first half of 2024, the data center sector investment activity increased by 185% year on year, reaching US$54bn in transaction volumes compared to US$19bn in the previous year. The biggest deal was the US$9.2bn equity raise by Vantage Data Centers, which saw investments from DigitalBridge and Silver Lake Partners. Other major deals included the US$3.3bn debt raise by STACK Infrastructures and US$3bn Edgeconnex European portfolio financing.

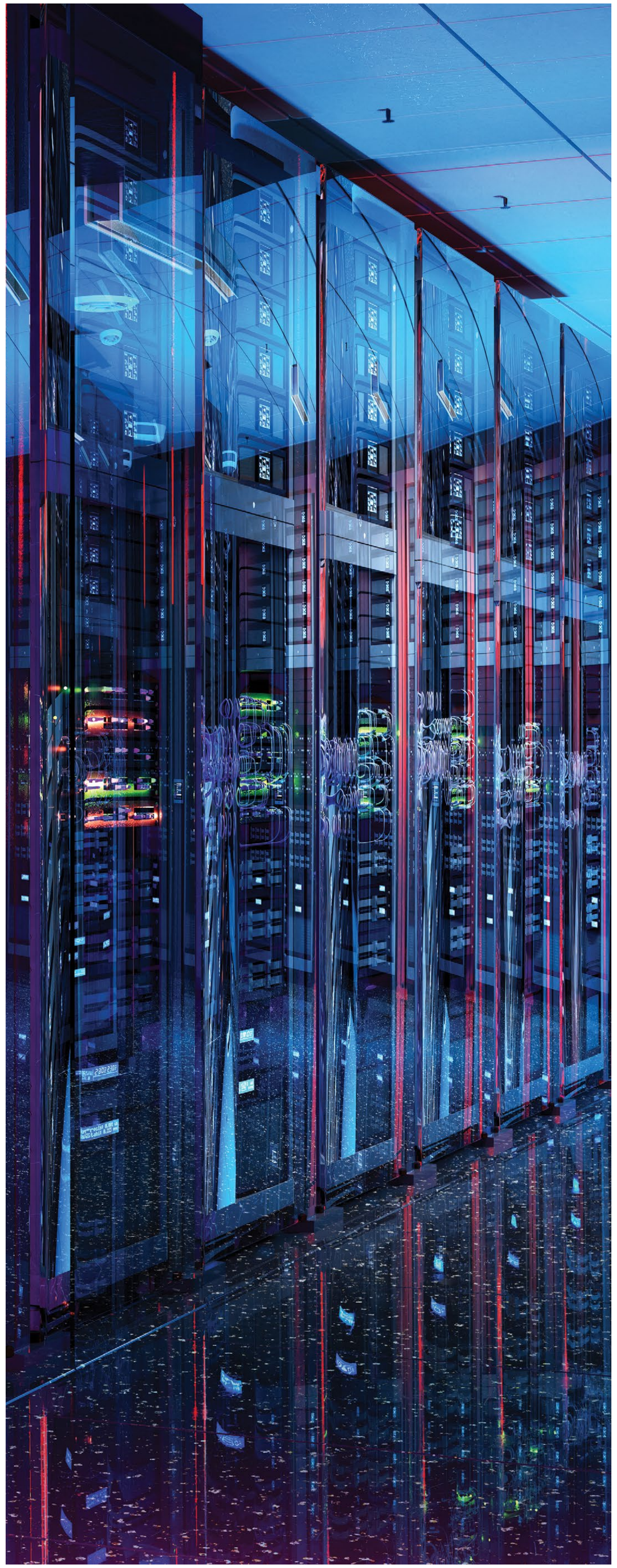
Hot topics.

Hot topics include:

- server virtualization
- edge computing
- data processing
- sustainability and energy efficiency
- climate litigation
- regulatory considerations such as data privacy and security
- technological advancements of AI
- investment trends
- site selection criteria
- infrastructure requirements
- risk management strategies

Server virtualization

Server virtualization is the usage of cloud software platforms to transfer and make information and applications accessible from physical data centers into digital data centers; in essence, dividing a physical server into segregated virtual servers. It is used in Software-Defined Data Centers (**SDDCs**) and offers companies multiple benefits; By using fewer physical servers, server virtualization can save resources and lower costs.



Regulatory considerations (power, data privacy, security)

Regulatory considerations come into play in data centers in several ways. Data center operators should be aware of the regulatory framework that applies to agreements with power suppliers, as an uninterrupted power supply is essential for performance. Moreover, onsite electricity generation may present an additional income stream, if certain regulations are observed when generating renewable energy from certain specific sources. It is crucial to understand these regulations before entering into agreements in the context of onsite energy generation.

Compliance with evolving data privacy regulations remains an important topic. Data centers are critical hubs of sensitive information and so are susceptible to cyber-attacks. These are increasingly more sophisticated and can create liability claims for data center operators by their customers. Operators should be aware of the applicable regulatory framework and required infrastructure to ensure data security. These requirements become increasingly important as the IoT collects an almost unlimited amount of data which is processed and stored at data centers.

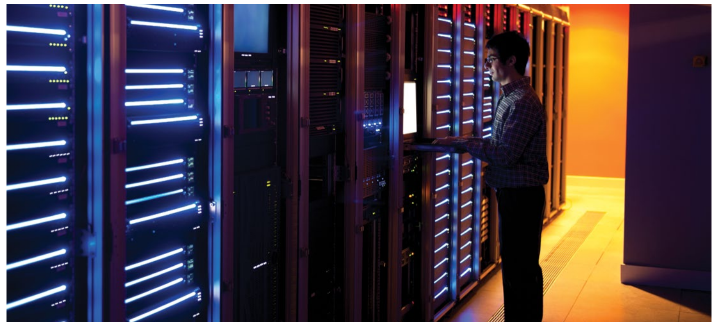
Technological advancements of artificial intelligence

Soaring Artificial Intelligence (**AI**) and reliance on cloud services will continue to push data center demand and growth. Companies may choose public or private cloud systems or both. 2025 will see the continued growth of high-performance multicloud architecture, which allows businesses to leverage multiple cloud service providers, private, public or hybrid, to optimize performance. It permits businesses to choose a specific geographic location and cloud provider according to their needs and in response to increasing costs, environmental disruptions and cyber-attacks. Relying on multiple cloud providers decreases security risks and can be more cost efficient if businesses strategically distribute their data.

AI development is powered by data centers which serve as its critical infrastructure. AI development also benefits data centers by enabling them to operate in a smarter, and more energy-efficient way, however the more data is stored to train AI Machine Learning (**ML**) and Large Language Models (**LLMs**), the more energy is consumed. Schneider Electric, a French multinational company, estimates that AI power consumption amounts to 4.5GW today, and will grow at a rate of 25% to 33% annually until 2028, when it could reach as much as 18.7 gigawatts.

On the plus side, AI data centres can have higher latency which opens up potential locations in new geographies away from the traditional core locations of Frankfurt, London, Amsterdam and Paris (**FLAP**).

While the main data center cooling practice is through air cooling and liquid cooling, in 2024 there has been an increase in AI utilization to increase the cooling efficiency of data centers while reducing the costs. Google utilized AI to achieve a 40% reduction in cooling costs, however, not only technological companies are using AI to reduce cooling costs. Equinix is one of the companies that through AI has managed to improve the energy efficiency of one of its data centers in Frankfurt, Germany.



Investment trends and funding opportunities

The industry has seen a substantial increase in the investment into and financing of the expansion of data center capacity and facilities, especially in the United States. In July 2024, CyrusOne, a Dallas based data center company, secured a US$9.7 billion credit facility to fund its data center growth. In June 2024, DigitalBridge Group, an asset management firm, and Silver Lake, a private equity firm, led an investor group in closing a US$9.2 billion equity investment in Vantage Data Centers.

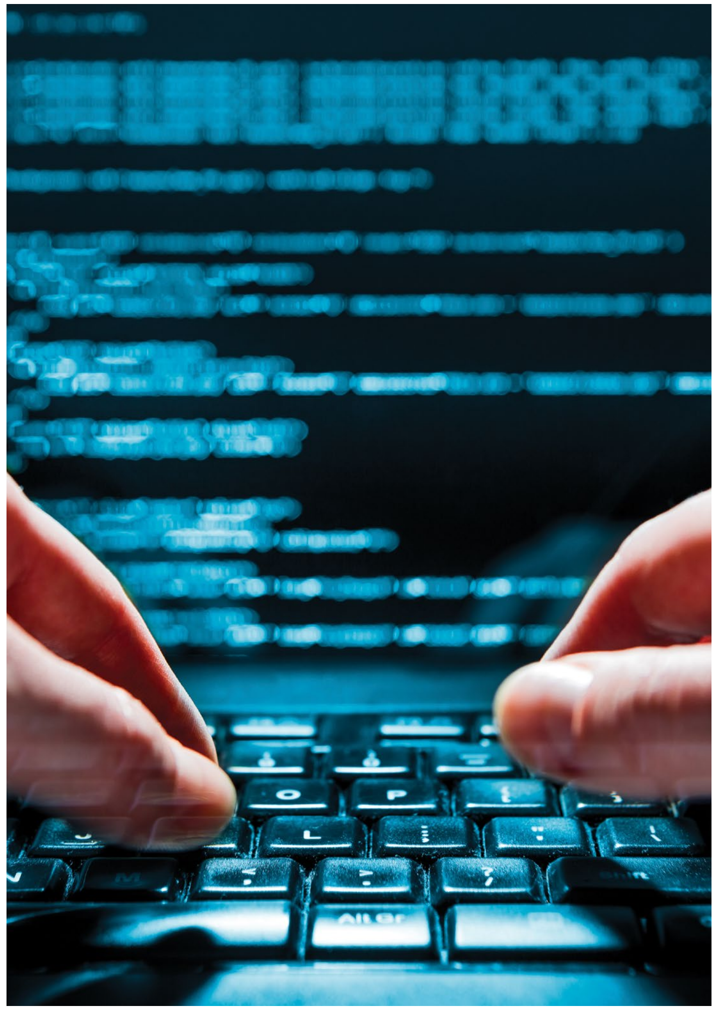
According to Infralogic the total closed transactions in data centers in 2023 amounted to US$61 billion, the total loan debt was US$33,5 billion and the total capital market debt was US$5 billion. In contrast, by Q3 2024, the total value of closed transactions amounted to US$72 billion, of which the total loan debt amounted to US$46.7 billion and the capital market debt is US$7 billion. This shows a notable increase in both equity investments and funding opportunities in the data centers market.

Infrastructure requirements

Infrastructure requirements are critical for the operation of data centers. One of the primary components is the physical structure itself, which must be designed to support heavy equipment loads and provide adequate cooling solutions. Data centers often require raised flooring systems to facilitate airflow and manage cabling effectively. Additionally, robust power supply systems, including Uninterruptable Power Supplies (**UPS**) and backup generators, are essential to maintain uptime during outages.

Cooling systems, such as Computer Room Air Conditioning (**CRAC**) units or liquid cooling technologies, play a vital role in dissipating heat generated by servers and maintaining optimal operating temperatures. Under the Uptime Institute standards, these qualify as Tier I data centers, and protect against disruptions from human error but not unexpected failure or outage.

Further, Tier I facilities, in particular, incorporate redundant capacity components for power and cooling systems that enhance maintenance opportunities and provide greater protection against disruptions. Key components of Tier II infrastructure include engine generators, energy storage systems, chillers, cooling units, UPS modules, pumps, heat rejection equipment, fuel tanks, and fuel cells. These elements collectively contribute to a robust environment where the distribution path can be maintained without requiring a complete shutdown of the system.



The Uptime Institute Tier System

The Uptime Institute created the Tier system for classification of data centers and are the international standard for data center performance, with progressive Tiers. A higher Tier doesn't make a data center better, it just means that it fits different business operations:

Tier I: protects against disruptions from human error, but not unexpected failure or outage. Redundant equipment includes chillers, pumps, UPS modules, and engine generators. The facility will have to shut down completely for preventive maintenance and repairs, and failure to do so increases the risk of unplanned disruptions and severe consequences from system failure.

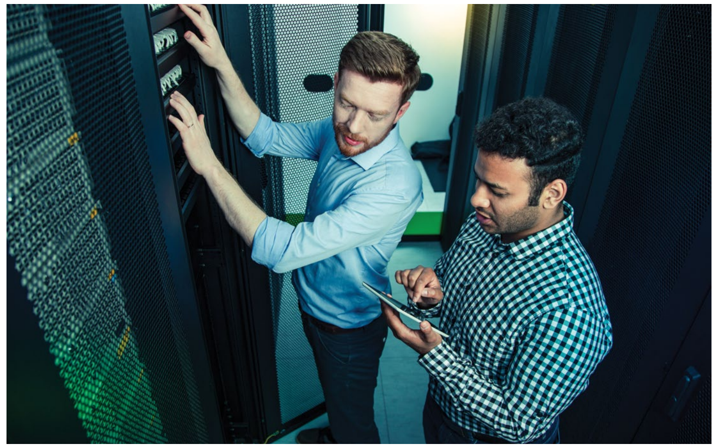
Tier II: includes redundant capacity components for power and cooling that provide better maintenance opportunities and safety against disruptions. The distribution path of Tier II serves a critical environment, and the components can be removed without shutting it down. Like a Tier I facility, unexpected shutdown of a Tier II data center will affect the system.

Tier III: concurrently maintainable with redundant components as a key differentiator, with redundant distribution paths to serve the critical environment. Unlike Tier I and Tier II, these facilities require no shutdowns when equipment needs maintenance or replacement. The components of Tier III are added to Tier II components so that any part can be shut down without impacting IT operation.

Tier IV: A Tier IV data center has several independent and physically isolated systems that act as redundant capacity components and distribution paths. The separation is necessary to prevent an event from compromising both systems. The environment will not be affected by a disruption from planned and unplanned events. However, if the redundant components or distribution paths are shut down for maintenance, the environment may experience a higher risk of disruption if a failure occurs. Tier IV facilities add fault tolerance to the Tier III topology. When a piece of equipment fails, or there is an interruption in the distribution path, IT operations will not be affected. All of the IT equipment must have a fault-tolerant power design to be compatible. Tier IV data centers also require continuous cooling to make the environment stable.

Risk management strategies

One of the primary strategies involves conducting comprehensive risk assessments to identify vulnerabilities related to physical security, environmental hazards, and cybersecurity threats. By evaluating factors such as location risks (e.g., natural disasters), equipment failure, and potential cyberattacks, data center operators can develop targeted mitigation plans. Implementing redundancy measures – such as backup power supplies, redundant cooling systems, and multiple internet connections – helps ensure that critical operations can continue even in the face of unexpected disruptions. By fostering teamwork and using effective risk management practices, data centers can enhance their resilience against potential disruptions while supporting overall business objectives.



ESG.

Data center energy efficiency

Data center developers and operators are having to accelerate energy efficiency measures to satisfy the ESG demands of their colocation tenants.

The exponential growth in demand for data center space (and power and cooling) is predominantly being driven by new technologies such as AI, the roll-out of 5G networks and the use of cloud computing. It is estimated that the increasing adoption of AI technology will lead to more than a doubling of global demand for electricity to power data centers by 2026 with some countries and regions experiencing unsustainable growth projections. For example, at the current rate of data center growth, Ireland will need to allocate around a third of its total electricity consumption to power its data centers by 2026.

Meanwhile, the data center tenants (which are increasingly dominated by the global cloud providers such as AWS, Microsoft Cloud and Google Cloud) have committed to challenging ESG targets, for example, AWS has committed to net zero emissions from 2040 and Microsoft Azure to using 100% renewable energy by 2025.

These two opposing trends have shone a spotlight on the efficiency of data center power use and the increasing need to develop more sustainable ways of powering and cooling data centers. The Power Usage Effectiveness (**PUE**) metric for data centers has been broadly flat over the last few years and there is a growing realisation that significant investment and the use of new technology and operational efficiencies will be needed in the coming decades.

In addition to the increasing demand for clean renewable power to power data centers, there have been successful trials in the UK and the U.S. to recycle the heat produced from server equipment to heat nearby homes and commercial buildings. Microsoft has also been trialling underwater data center technology which could be used for small scale 'edge computing' deployments. "Regulatory frameworks are now being adopted to encourage more sustainable data center facilities. For example, the European Commission's Joint Research Centre **(JRC)** , has developed the *EU Code of Conduct (CoC) for Data Centers* which is a voluntary framework for data center operators and owners to adopt best practices that reduce energy consumption and promote sustainability to meet the EU's net zero requirements.

It is clear that the demand for data center space is only going to dramatically increase over the coming years as emerging technologies utilise scarce resources and so the data center tenants' requirements for better PUE and cleaner energy and cooling solutions will become more demanding as they struggle to meet their own ESG commitments.

Climate litigation risks

Climate-related litigation has rapidly grown in recent years, and we see new risks and types of claims emerging all the time.

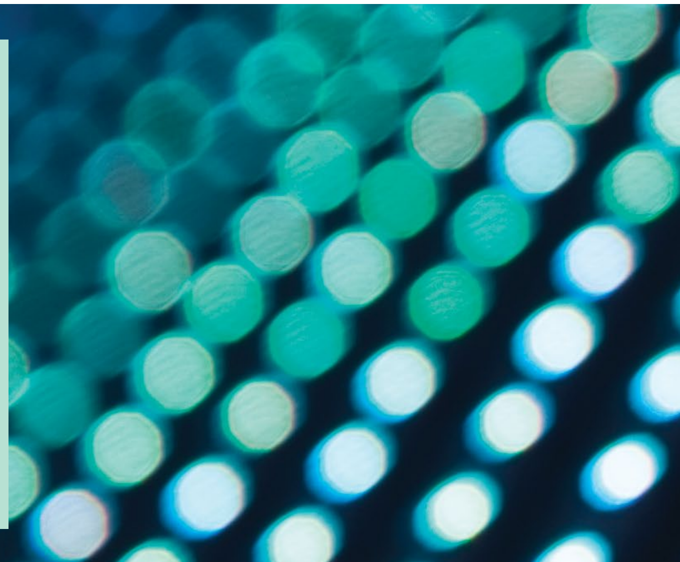
As a category, climate litigation covers a multitude of actions brought before administrative, judicial and regulatory and investigative bodies, raising a huge variety of issues of law and fact regarding (but not limited to) our changing climate. It's not only traditional "carbon majors" who face climate litigation risk – changes in climate law plaintiffs' approaches, as well as shifts in the regulatory landscape, mean that climate litigation is brought against an increasingly wide range of participants in the business ecosystem.

Claims can take lots of different legal forms, including, for example, tort (negligence and nuisance claims), corporate law (e.g. corporate liability for alleged climate harm), breach of fiduciary duty (e.g. failure to manage or disclose climate risks), consumer law (e.g. misrepresentation, greenwashing), and statutory planning regimes (e.g. challenges to granted planning permissions) – to name just a few. The number and variety of these claims are only expected to grow further as successful cases emerge and generate yet more momentum.

Increasing awareness of the environmental load produced by digital-centric businesses may lead climate activists and other claimant-side actors to focus on the environmental footprint of service-providers to industry, such as data centers. For companies operating in the data center sphere, be it businesses that use data centers or the operators themselves (if separate), climate litigation presents tangible risks in terms of physical operations, real estate portfolio, investment decisions, net-zero transition journey and associated shifts in the regulatory, technological and stakeholder landscape in which they operate.

Although such risks are far-reaching, feasible safeguarding options for mitigation and adaptation are already available (e.g., internal policy development, contractual safeguards, horizon scanning, involvement in policy debate, responsible lobbying, etc.) and we are on standby to support our clients in successfully navigating climate litigation risks.

These two opposing trends have shone a spotlight on the efficiency of data center power use and the increasing need to develop more sustainable ways of powering and cooling data centers.



Considerations for investors and developers.

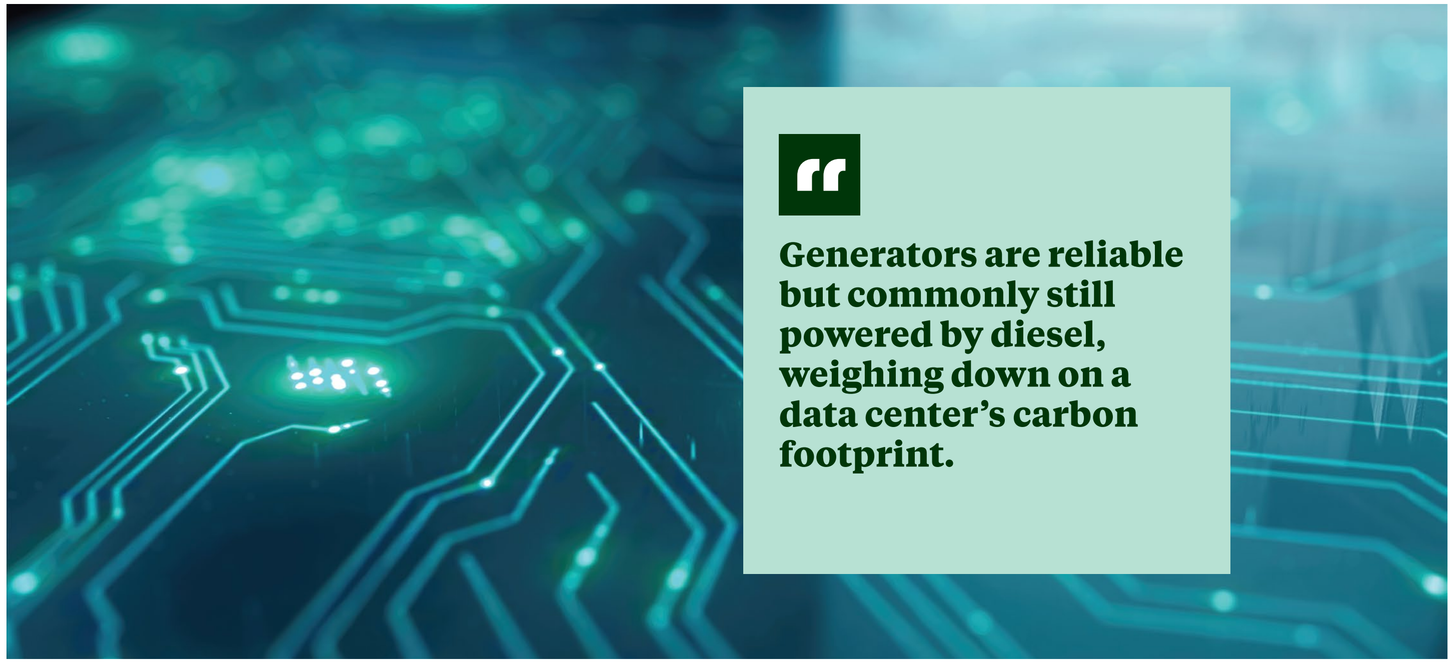
Location

The choice of location of a data center is paramount for almost all other aspects of operating it, particularly the possibility of connecting it to a power grid, compliance with regulatory requirements and proximity to customers. Other criteria, such as security measures and costs also play a role in deciding where to operate a data center. The determining factors for choosing a location derive from both the internal requirements and the environment surrounding the data center. To ensure that a data center is set up for success, we can advise you on choosing the right location for your needs. A preliminary risk analysis can help identify risks deriving from the geographical location and eliminate hazardous locations, and also to identify planning/zoning issues and availability of tax incentives/financial grants.

A) Grid connection

Power supply is of utmost importance for the operation of a data center and must be reliable and secure. With up to 50% of a data center's operational expenses going toward electricity, selecting the right power supply strategy is critical for both operators and tenants, especially in powered shell solutions. Understanding and securing reliable and cost-effective energy sources is essential to ensuring uninterrupted operations. Data center operators have several key options for meeting their energy needs:

- Full Supply Contracts: Engage directly with an energy supplier to cover all energy requirements. This option offers simplicity and predictability, with a single point of contact for energy procurement and management.
- Power Purchase Agreements (**PPAs**): Enter into direct agreements with energy producers, eliminating intermediaries. PPAs can provide long-term price stability and are particularly beneficial when sourced from renewable energy providers, contributing to sustainability goals and potentially offering financial incentives or tax benefits.
- Market Procurement: Purchase energy on the open market through Over-The-Counter (**OTC**) contracts or via the energy exchange. This approach allows operators to take advantage of market fluctuations, but it requires a sophisticated understanding of energy markets and carries some risk due to price volatility.
- Onsite Energy Production: Generate electricity on-site using renewable or conventional energy sources. This option offers greater control over energy supply and can enhance resilience against grid outages. However, it requires significant upfront investment and ongoing maintenance.
- Direct Wire: Direct link to a power station or source, cutting out the network operators and providing cost benefit and certainty, and redundancy.



Generators are reliable but commonly still powered by diesel, weighing down on a data center's carbon footprint.

In addition to these options, it is essential to consider other power supply factors, such as resilience, grid connectivity and energy efficiency. In order to prevent downtime during power failures and cyber-attacks, backup power systems, such as generators and uninterruptible power supplies should be put in place. Before deciding where to locate a data center, the reliability of the local grid should be evaluated and ideally include dual-feed power supplies for additional security. Implementing energy-efficient technologies and practices reduces overall costs and contributes to operating more sustainably.

Nonetheless, the power supply of a data center may be interrupted. To minimize the damage from such interruptions, certain measures can be taken from the beginning and should be included in agreements even prior to construction or lease of a data center. Some common backup power options include backup generators, batteries and UPS systems. Generators are reliable but commonly still powered by diesel, weighing down on a data center's carbon footprint. UPS systems immediately restore power during an outage, using stored energy to maintain a continuous power supply. It is important to consider, whether a data center needs multiple backup systems and which ones are preferrable for a specific data center.

B) Regulatory considerations

Regulatory compliance is required throughout the process of designing, constructing or leasing and operating a data center. Depending on the respective stage, different regulations come into play. First, data centers cannot be operated in all areas, and certainly not constructed everywhere. Restrictions on planning/zoning are critical to understand, and for developers, present the opportunity to amend planning frameworks. Certain locations may present a hazard, such as chemical and nuclear energy plants, airports, of course any area with flood risk, and also critical national security infrastructure (if for no other reason than it may impact liquidity). The German Federal Office for Information Security, for example, issues guidelines on the geographic considerations and restricted areas for data centers in Germany. Secondly, if an area is available, building permits and environmental assessments are usually required before construction can begin. The process of obtaining the necessary permits can be cost intensive, and should not be underestimated – and they can also be very slow to obtain. Thirdly, additional regulations on fire security will need to be met as data centers usually generate extreme levels of heat. Lastly, once the data center begins operations, data privacy, environmental, and product liability regulations apply.

Design requirements

Data centers require specific design considerations as compared to other building designs to ensure successful operations later. Managing and housing critical IT infrastructure warrants reliability, scalability and efficiency. Some key topics to cover in lease or construction agreements are cooling systems, access control and fire security.

A) General design requirements

Depending on the level of reliability, data centers are qualified as one of four Tiers, Tier I being the least reliable and Tier IV being the most reliable. (see page 7 for more details setting out the Uptime Institute's classification). The Tier is determined by the infrastructure in a data center and can be improved by increasing the redundancy of its components, efficiency, sustainability and security. Planning and installing multiple fiber paths, for instance, can help prevent single points of failure and ensure continuous operations. Data centers require more robust electrical infrastructure than other commercial building types. They are also often required to scale up or down to meet fluctuating needs. Environmental monitoring should already be considered in the planning stages, with extreme levels of heat requiring increased airflow and cooling.

B) Access control

Data centers are the backbone of a lot of critical IT infrastructure and must ensure adequate security measures. Access control measures, such as surveillance technologies, should be included in the design plans. Other physical measures include hiring security personnel for the site, maintaining an access list of every person authorized to enter certain areas onsite and installing secure access points. Perimeter security can be achieved by installing tall fences around the site and constructing the building in a non-descript manner, preferably without windows. Machinery such as UPS and generators should be protected separately, for example by concrete walls. Metal detection screening can be installed at entrance points to the data center floor and between different compartments if several tenants are leasing space within the same building.

Similarly, before leaving the facility, a final security checkpoint can be installed. High-level security technology including two-factor authentication checkpoints using biometric data are available for tier 3 and tier 4 data centers. The levels and combinations of access control may vary, depending on the tier of the data center.

C) Power usage effectiveness

To assess the efficiency of Heating, Ventilation, Air Conditioning (**HVAC**) systems in data centers, Power Usage Effectiveness (**PUE**) was introduced. It measures a data center's overall energy consumption against the energy used by IT installation, with the highest PUE score marking that all consumed energy is used to power the IT infrastructure. Design strategies can contribute to improving the PUE metric by reducing energy consumption.

D) Cooling systems

Typical methods for cooling include air conditioning, hot aisle/cold aisle and liquid cooling systems.

The hot aisle/ cold aisle method involves the CRAC (computer room air conditioning) streaming cold air out of grids in the floor and pulling it through the servers, then discharging the collected hot air into the hot aisle and letting it lift to the ceiling, pulling it back and repeating the process. While it helps cool down the servers, there is a risk of cool and hot air mixing.

Liquid cooling systems are less cost-intensive and more efficient. Two main systems of liquid cooling are commonly used: immersion cooling and direct liquid cooling. When using immersion cooling, servers are fully or partially immersed in a dielectric liquid which removes the heat and releases it through either a single-phase or two-phase system. There are various sub types of immersion cooling that designers can choose from, depending on their priorities. Direct liquid cooling establishes a cooling loop where the dielectric liquid absorbs heat from components through conductive metal plates. Like in immersion cooling systems, direct liquid cooling is possible as a single-phase and two-phase technology.

E) Fire security

As data centers generate extreme levels of heat, they are highly vulnerable to fires. Fire protection is a critical component of design agreements. In order to detect a fire at its inception, installing smoke detectors is an important measure. Additionally, heat detection systems should be installed to identify heat anomalies and signal potential fire threats. If a fire breaks out, several suppression mechanisms can be employed to minimize the damage. Designers have a choice between using gas or chemicals and water-based suppression, such as sprinklers and water mist systems. When planning the design of a data center, fire security can influence the layout. Compartmentalizing the data center into different zones can help contain a fire. Integration with the building's cooling system can also prevent the spreading of a fire by providing additional suppression mechanisms.

> **Depending on the level of reliability, data centers are qualified as one of four tiers, tier one being the least reliable and tier four being the most reliable.**

Building or leasing a data center

One of the principal decisions to be made is whether to build or lease a data center. Building a data center offers increased customization, allowing for specifications. However, it may come at a higher cost than leasing as it requires substantial upfront capital investment in addition to fees for architects, planning and design costs, and more. Building and using also eliminates the risk of potentially losing a lease. Vice versa, leasing a data center can grant immediate access to a site and accelerate the start of operations. Building a data center allows the owner to lease parts to tenants and generate revenue. From a tenant's perspective, on the other hand, a lease should include controls on the other potential tenants who might share the space. A lease agreement may also be combined with elements of a service agreement, to allow for a hybrid model integrating leased and service-based resources.

A) Data center leasing agreements

If the decision is made to lease a data center, various forms of lease agreements are possible:

- Wholesale data center;
- Powered shell;
- Colocation (**Colo**) solutions;
- Server hosting – managed hosting;
- Cloud computing;

The right choice for a tenant depends on the specific driver(s). If the cheapest solution is needed, a pure hosting structure may be more favorable than a wholesale or colocation structure. Colocation structures offer increased scalability and wholesale solutions may result in lower expenditure because a larger space is usually leased long-term. However, size is an important factor also. Wholesale data centers tend to suit the larger user. Traditionally, the user would be the only occupier and have exclusive access, although may have to commit to a minimum power usage requirement. The hosting/retail colocation solutions tend to suit smaller users. Hybrid solutions are also possible and offer flexibility to tenants. Powered shells are data centers that are delivered with unfinished interiors, but with power and connectivity, for the tenant to fit out. In recent practice, we have seen more Built-to-Suit **(BTS)** models whereby the tenant strongly influences or determines the design of the building. Those hybrid models provide various interface issues in practice and require clear legal documentation.

Data center leases commonly warrant a number of specific agreements to accommodate the needs of tenants and landlords alike. The lease agreement is usually the principle document to govern their relationship and must therefore be carefully drafted. Some of the key topics to consider in more detail are:

- Lease term and renewals
- Space and permitted uses
- Maintenance and repairs
- Power supply and cooling systems
- Connectivity
- Liability and indemnification
- Security and access
- Nature/identity of other occupiers
- Service levels
- Expansion and contraction

Initial terms typically range from 15 to 20 years, so an occupier needs to understand what would benefit it best if it is going to lease space as opposed to a hosting solution. The number of renewal periods should also be considered, as well as any pre-emption rights that the tenant may hold. Including pre-emption rights may increase the flexibility and security of the lease for tenants.

Similarly, lease agreements should provide flexibility for the tenant to scale operations throughout the leasing period, for instance by expanding operations. The lease agreement should provide for scenarios in which the tenant needs additional space for equipment and infrastructure, and what the landlord will commit to provide.

The lease agreement must clearly define

the responsibilities for setup, alterations, maintenance, repair, and replacement, depending on ownership and obligations concerning the facility's infrastructure. These will often be marked to International Standard Organization (**ISO**) standards. Specific provisions should address who is responsible for making alterations and performing maintenance or repairs, as well as the replacement of critical systems. Both the tenant and the landlord may need to adhere to certain standards and maintenance schedules. Additionally, the agreement should include detailed provisions regarding services related to data center equipment, heating, ventilation, and other essential infrastructure. Power supply and cooling systems must also be regulated in a data center lease agreement. Uninterrupted power supply is the foundation for data centers, as is an efficient and cost effective cooling system. The parties should agree on percentages of agreed availability and describe contractual services in a sufficiently detailed manner, in order to prevent later conflicts in cases of outages. Depending on the type of lease agreement, the tenant (powered shell lease agreement) or the landlord may be responsible for installing the cooling system.

Including a limitation of liability clause can be advantageous for both parties, protecting them from excessive risk in the event of unforeseen circumstances. The agreement should also comprehensively address data protection and security, including stringent protocols for physical access to the building and IT systems, as well as compliance with applicable laws and regulations, such as GDPR or other relevant data protection legislation. Indemnification clauses should be included to protect each party from potential claims arising from breaches and other liabilities related to data protection and security, specifically.

To handle data breaches efficiently, clear procedures for responding to them should be established in the agreement, including notification requirements and remedial actions. Insurance requirements may also be covered by the agreement, particularly for cases of data breaches and protection of property.

Data breaches can be prevented and their consequences can be minimized with an adequate security concept. Physically, access to the building should be regulated in the lease agreement, as well as employing security personnel and installing a surveillance system. Virtually, the responsibility of landlord and tenant for encrypting data and putting measures in place to protect that data center's network are critical. Investigation and remediation after a breach are equally as important. Regular security audits can help assess the effectiveness of the security concept and identify weaknesses.

Two primary options are available: utilizing multiple contractors with a potential designer or engineer (multi-lot approach) or opting for a turnkey solution where an EPC contractor assumes full responsibility for the project.

B) Construction agreements

Construction agreements cover different topics, depending on whether a data center is a brownfield or greenfield project. Unlike brownfield projects, developing greenfield data centers – or even expanding existing ones – presents unique challenges and risks, particularly when it comes to delivering the project on time (planning and zoning risks being critical to understand) and within the pre-agreed budget. Developers must carefully choose the right approach.

i. Turnkey or multi-lot approach

Two primary options are available: utilizing multiple contractors with a potential designer or engineer (multi-lot approach) or opting for a turnkey solution where an Engineering, Procurement and Construction (**EPC**) contractor assumes full responsibility for the project. Both offer advantages and disadvantages. A multi-lot approach that engages multiple contractors and a designer or engineer can offer a more cost-efficient solution. This approach allows for greater flexibility in selecting specialized contractors for various project components. However, it requires the developer to manage multiple interfaces, coordinate various stakeholders, and assume more significant risks related to integration, timelines, and cost control.

Choosing a turnkey EPC contractor, on the other hand, transfers the responsibility for the entire project to a single entity, covering engineering, procurement, and construction. The EPC contractor assumes full responsibility for completing the project, managing risks, and ensuring the project is delivered as a ready-to-operate facility. This approach offers the advantage of having a single point of contact and accountability, simplifying project management and reducing the complexity of coordinating multiple role players. One of the most significant benefits of the EPC model is having a single entity responsible for the project's completion, mitigating the risks associated with managing multiple contractors and interfaces. The EPC contractor bears the full turnkey and interface risk, which is particularly valuable in highly complex projects like data centers. While the EPC contractor may engage various subcontractors for specific tasks, the contractor remains directly accountable for delivering the project. However, all these benefits come at a price, as the contractor expects to be rewarded for the assumption of risk.

ii. Infrastructure management

Often, the end user is a tenant of the party who developed the data center. They have a critical interest in the compatibility of all components. Data Center Infrastructure Management (**DCIM**) refers to coordinating and managing interactions between various stakeholders involved in the construction, design and operation process. The various interfaces and connections in a data center environment are typically monitored and controlled by various tools and processes. This includes the physical and virtual space and covers storage devices, servers, network equipment and other components. DCIM is crucial for maximizing performance. Including DCIM in an agreement allows for clearly allocating responsibility. It should cover the scope of work, standards and protocols, performance metrics and reporting requirements.

Our capabilities.

The value we bring to clients is both in the depth of expertise in critical subject areas in every aspect of data center development, leasing, financing, and operation, and also in the understanding of the regulatory issues that affect them. Our dedicated data center team brings together all the skills of a multi-disciplinary, international firm.

Experience

- ***Keppel DC REIT*** on the acquisition of a data center in the Netherlands
- ***Stumpf Group*** on a minority investment by funds managed by BDT Capital Partners in Exyte Group
- ***Pantheon***
  - as co-lead investor on €1.4bn Goldman-seeded credit fund
  - as co-lead investor in CAD$1.8billion technology data center transaction
- ***Du Pont Fabros Technology*** on its US$7.65bn sale to Digital Realty, creating the largest wholesale data center REIT in the United States
- ***Rolls-Royce's Power Systems division***, one of the top three suppliers of backup power systems for data centers, on the conclusion of a long-term contract for the procurement of fuel cell modules from cellcentric
- ***Colohouse***, a colocation, cloud, hosting and network services company in connection with
  - the acquisition of Hivelocity, a leading provider of bare metal services
  - the acquisition of Steadfast, a cloud, bare metal and data center provider
  - the acquisitions of Data102, and Turnkey Internet data centers, colocation businesses, and bare metal services
  - the acquisition of the business and data centers of Interconnect Miami, a colocation and data center provider
  - the acquisition of Lume Cloud, a managed cloud services provider
- Mapletree Investments on a US$1.4bn acquisition of a data center portfolio in North America from Digital Realty Trust
- ***QTS Realty Trust*** on a US$10bn acquisition by Blackstone
- ***Founder, Robin Khuda***, on partial sale of his interests in data center business AirTrunk (valued at approximately A$3bn) to MIRA, together with consortium arrangements with MIRA
- ***fifteenfortyseven Critical Systems Realty (1547)*** a developer, operator and owner of highly-interconnected data centers with over 1.25m sq. ft of data center space in North America under management, in connection with the following acquisitions and joint ventures
  - joint venture with another data center fund for AlohaNAP located in O'ahu in Hawaii
  - the acquisition with another data center fund of the Global Access Point Union Station in South Bend
  - the acquisition with another data center fund of Chase Tower in McAllen, TX, a hub for telecommunications traffic between Mexico and Texas
- ***International lending consortium*** on a €1bn+ data center platform financing for Maincubes
- ***Digital Transformation Capital Partners*** on a large-volume investment in German colocation data center operator Maincubes
- ***AtlasEdge*** on the acquisition of Datacenter One
- ***BlackRock*** on the financing supporting the acquisition of InfraData by IK Investment Partners
- ***NorthC Group***, the leading Dutch regional colocation provider
  - on the acquisition of the German colocation provider IP Exchange GmbH
  - on the acquisition of Netrics connectivity services and data centers
- ***Ascendas REIT***, a CapitaLand sponsored REIT and Singapore's first and largest listed business space and industrial REIT, on its €555m acquisition of a portfolio of 11 data centers from Digital Realty Trust. The portfolio comprises 11 facilities, four in the United Kingdom, three in France, three in the Netherlands, and one in Switzerland. This transaction marks Ascendas REIT's first European data center acquisition
- ***Infratil***, the listed vehicle of the New Zealand based infrastructure fund Morrison & Co, on its £130m investment in a 40% stake in the Kao data center in Harlow
- ***PCCW*** on the sale of its multiple-site data center business across Asia to DigitalBridge
- **Mainova WebHouse GmbH** on €475 million financing for data center projects in Frankfurt.

Our team.

Our data center team, which stretches from the west coast, across Europe (especially FLAP) and through to Asia, works together to coordinate this advice across jurisdictions, exercising sound judgment in supporting clients with location selection decisions and strategies for successful project development and execution; and shares experience on SLAs, KPIs, service obligations and leasing terms across the international network.

Our global center team is made up of experienced projects, real estate, corporate, regulatory, product liability, privacy and cybersecurity, commercial and finance lawyers who can assist with all aspects of the acquisition (direct or indirect), pre-letting, development and construction of data centers/ development sites and key operational issues around services, suitability/ownership of site, planning and environmental issues, and ownership and supply of key infrastructure (e.g. power (and particularly the key question of whether reserved supply will actually be available on completion of a development), cooling, fire suppression, data transmission and redundancy).

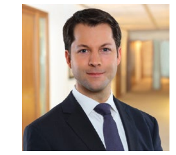
EMEA


Lauren Bruce
Infrastructure and Projects
London


Maximilian Broermann
M&A
Frankfurt


Xavier Doumen
M&A
Paris


Tobias Faber
Infrastructure and Projects
Frankfurt


Markus Franken
Real Estate
Frankfurt


Luke Grubb
Strategic Operations
London


Martin Haase
Real Estate
Dusseldorf


Sian Howes
Real Estate
London


Anna-Katharina Friese-Okoro
Intellectual Property,
Hamburg


Valerie Kenyon
Product Liability
London


Clare King
Real Estate
London


Charlotte Le Roux
Strategic Operations
Paris


Carla Luh
Infrastructure and Projects,
Hamburg, Frankfurt.


Daniel Norris
Real Estate
London


Sarah Shaw
M&A
London

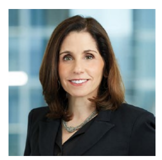

Rosie Shields
Real Estate
London

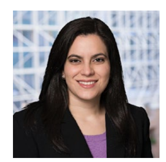

Eshana Subherwal
Product Liability
London

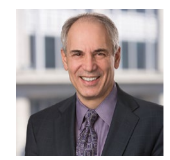

Scott Tindall
Infrastructure and Projects
London

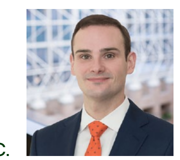

Lucy Ward
Product Liability
London

Americas


Loryn Arkow
Real Estate
Los Angeles

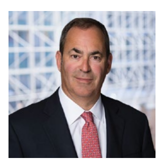

Elizabeth Akerman
Real Estate
New York

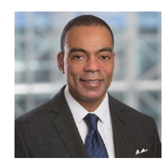

Lee Berner
Real Estate
Washington, D.C.


Michael Bonsignore
Infrastructure and Projects
Washington, D.C.

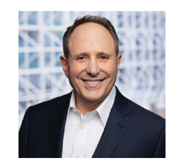

Chip Cannon
Global Regulatory
Washington, D.C.


Zenas Choi
Intellectual Property
Northern Virginia

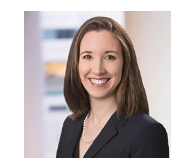

Brian Diamond
Real Estate
New York


Ari Fitzgerald
Communications Regulatory
Washington, D.C.

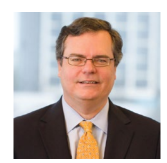

Lee Ann Fowler
Real Estate
Denver


Jeff Keitelman
Real Estate
Washington, D.C.


Fernando Margarit
Infrastructure and Projects
Americas
Miami


Stacey McEvoy
M&A
Washington, D.C.


Scott Reisch
Global Regulatory
Denver


Robert Welp
Private Equity
Northern Virginia

APAC


Matt Bubb
Infrastructure and Projects
Singapore


Thomas Kim
Private Equity
Singapore


Derrick Lau
Banking
Hong Kong


Louise Leung
Banking
Hong Kong

Americas

- **Boston**
- **Denver**
- **Greater Washington, D.C.**
  - Baltimore
  - Washington, D.C. and Northern Virginia
- **Houston**
- **Los Angeles**
- **Miami**
- **Minneapolis**
- **New York**
- **Philadelphia**
- **Northern California**
  - San Francisco
  - Silicon Valley
- **Latin America**
  - Brazil
  - Mexico

Europe, Middle East and Africa

- **Amsterdam**
- **Brussels**
- **Dublin**
- **Germany**
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- **London**
- **Luxembourg**
- **Madrid**
- **Milan**
- **Rome**
- **Paris**
- **Middle East**
  - Dubai
  - Riyadh

Asia Pacific

- **Greater China**
  - Beijing
  - Hong Kong
  - Shanghai
- **South East Asia**
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- **Tokyo**

www.hoganlovells.com