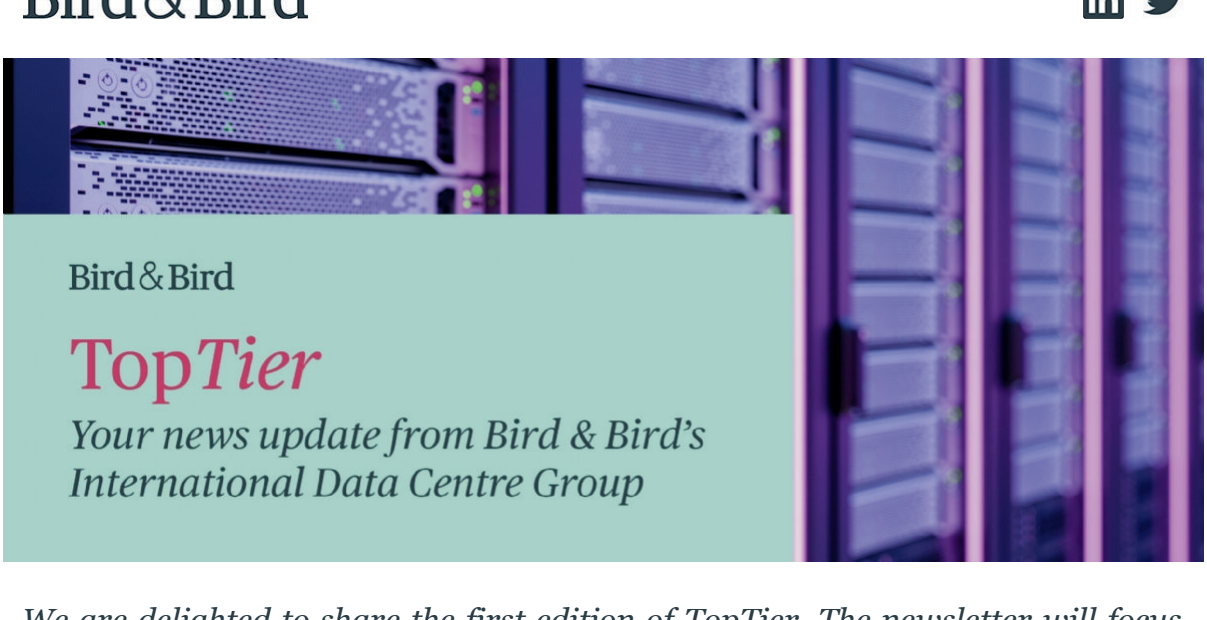
Bird & Bird



We are delighted to share the first edition of TopTier. The newsletter will focus on hot topics and legal development impacting various aspects of the data centre industry.

This issue has been edited by Marco Nicolai and Sophie Phillips with contributions from the Data Centre's team.

In this edition, we review the shift towards sustainable power solutions from regulations to practical change, the strengthened cybersecurity obligations across some key regions, new Spanish regulations, and colocation agreements. We further look at the increasing challenges for data centre construction and proven tools to address risks. Please **get in touch** if you would like to discuss any of the issues raised in these articles, or **visit our webpage** for more information about Bird & Bird's International Data Centre Group.

We hope you enjoy this first edition and look forward to the next one.

Click on the links below to jump to the respective article:

Contents

1. Powering the future: renewable energy and hydrogen
2. Data centres and cybersecurity
3. New Spanish regulations
4. Colocation – lease or licence?
5. Early contractor involvement (ECI)
6. Utilizing collaborative contracts

Sign up for our quarterly Data Centres updates

Powering the future: renewable energy and hydrogen for data centres

Data centres stand as the backbone of modern technology, enabling countless services and applications. However, this exponential growth in digital infrastructure comes with a significant energy demand, despite efficiency improvements in IT hardware and cooling systems. A shift towards sustainable solutions, including renewable energy sources and potentially hydrogen to power these data centres, is necessary.

The growing environmental impact of data centres

Data centres represent 3% of the energy consumption in the world (416 TWh). In 2030, they could represent more than 10% - if nothing is done. The growth of the sector shows the necessity for a big change regarding the energy sources fuelling these data centres.

From voluntary commitments to a regulatory compliance

Industry leaders are well aware of this situation and have already started to improve their sustainability record by reducing their carbon footprint and their energy consumption. The EU Code of Conduct for Data Centres [1] further encourages such voluntary adherence to best practices. But it's not only a voluntary commitment on a pilot project stage as the European and US legislators have already imposed regulatory compliance. Just a few recent examples:

European Union (EU)

1. Energy Efficiency Directive (EED)[2]:

- The EED sets out binding measures to promote energy efficiency and reduce energy consumption across various sectors, including data centres.
- Obligations under the EED include conducting energy audits, implementing energy efficiency measures and reporting on energy consumption and savings. Compliance is not only subject to penalties but will be a key element in commercial contracts and a competition factor between data centres. It will also impact the financing of such assets as ESG criteria become a crucial factor in loan agreements.
- The Commission Delegated Regulation on the energy efficiency of data centres and a dedicated rating scheme was published on May 17th 2024 and will enter into force on June 6th 2024. The delegated regulation defines the information that data centres with an installed computing capacity of more than 500 kW must provide to the European database. Operators must submit this information no later than 15 September, then 15 May 2025, and every year thereafter in order to build the future sustainability rating system for these facilities.
- Germany has been the first country to transpose the EED through its energy efficiency law [3]. Data centre operators have to decrease their "Power Usage Effectiveness" for new and existing data centres. With respect to renewable energy use, data centres are increasingly obliged to source electricity from renewable sources. From 2024 they must source 50% of their energy from renewable sources and from 2027 this obligation will be 100% renewable energy sourcing! Data centre operators can demonstrate compliance by using a "certificate of origin (GoO)" for the energy used. Data centres will become major purchasers in the commercial Power Purchase Market and the trend will increase on a European and international level.

2. Renewable Energy Directive (RED)[4] :

- The third version of the RED directive published in 2023 establishes binding renewable energy targets for EU countries and sets out measures to promote the use of renewable energy sources.
- Industry should increase the use of renewable energy by 1.6% per year. The EU Member States have also agreed that by 2030, 42% of the hydrogen used in industry should come from renewable fuels of non-biological origin, going on 60% by 2035.
- Data centres may be encouraged or required to source a certain percentage of their energy from renewable sources to comply with the directive.

From regulation to practical change:

I. Renewable energy procurement through Corporate Power Purchase Agreements (PPAs) for data centres

Data centre operators are today (and will be obliged in future) securing renewable energy by agreeing Corporate PPAs with renewable energy producers. Those contracts are not easy to navigate through, they are long term, complex agreements, often with a financing angle, as the electricity producer will have to finance its (newly built) installation. Key challenges include contract duration, mutual (bank or parent company) guarantees based on respective counterparty risk assessment, termination grounds and liabilities. Foremost the data centre operator has to secure the correct issuance and ensure correct transfer of the guarantees of origin (or comparable environmental attributes).

Such transfer of guarantees of origin can today be made on a cross border basis. Such transfer will become increasingly important as data centres will operate under different jurisdictions and it can be of utmost importance to contractually secure the flexibility to transfer guarantees from one country to another to ensure regulatory compliance for each of an operator's respective data centres.

However, renewable energy production is often dependent on exterior factors such as wind power or sunlight. In order to maintain a reliable energy source at any time, hydrogen could represent an alternative power and storage solution in the future.

II. The role of green hydrogen in data centres

Interest in using green hydrogen, produced by decarbonized or renewable energy sources as a replacement for diesel back-up generators, and ultimately as a primary power source for data centres, has risen in the past few years.

When considering the opportunities for hydrogen in powering data centres, it is important to consider the difference between using the hydrogen as an energy storage system or as an energy generation system. In addition, it is crucial to carefully follow the EU and International requirements in order to ensure that the hydrogen qualifies as green or low carbon hydrogen.

The potential of hydrogen for data centres typically falls into the energy storage category, where electricity (from renewable sources) is utilized to generate low-carbon or green hydrogen which in turn is transported and stored before being converted back into electrical energy whenever needed. Two potential methods for converting hydrogen back to electrical energy are hydrogen fuel cells and hydrogen-powered gas turbines.

Fuel cells are well-suited for smaller-scale applications, such as replacing diesel generators in single facilities, while turbines excel in generating high megawatt outputs.

Typical data centre power autonomy comprises 24 to 48 hours' fuel storage. The diesel generators have to be tested regularly – and this requires diesel consumption just for testing purposes alone. Not very important on an individual data centre basis but significant on a global level. A growing number of data centre operators would like to end their reliance on diesel fuel for emergency backup power. Hydrogen is being advanced as a possible successor to diesel fuel generators.

The space requirement for hydrogen deployment is at least 2.5 times larger than that required for diesel back up generation, while capital expenditure could be five times greater or more. With the increasing push towards achieving net zero, it is widely expected that both the capital expenditure and footprint requirements for green hydrogen energy storage systems will decrease.

This decrease, together with the significant government and private investments, may continue to sway the balance in favour of hydrogen to decarbonize data centres.

For more information, please contact Sibylle Weiler.

[1] EU Code of Conduct for Energy Efficiency in Data Centres
[2] DIRECTIVE (EU) 2023/1791 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast) (the "Energy Efficiency Directive")
[3] German Energieeffizienzgesetz (EnEfG) from 20 October 2023
[4] DIRECTIVE (EU) 2023/2413 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 October 2023 amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652

New Spanish regulations – mandatory financial guarantees to the access and connectivity permits to develop a data centre in Spain

On 28 December 2023, Royal Decree-Law 8/2023 of 27 December 2023 was published ("**Royal Decree-Law 8/2023**"). This new provision affects the development of data centres in our country as they are facilities with a significant energy demand.

The number of data centres is growing exponentially in our country, especially since 2022. However, this new regulation imposes an obligation on those companies owning data centres that have already obtained their grid access and connection permits, which are essential for obtaining the huge amount of energy needed to carry out their activity.

Royal Decree-Law 8/2023 introduces in its third transitional provision the obligation to present guarantees for access and connection permits for demand facilities that have already been granted such permits. This requires that the connection point for which the permit has been granted must be at a voltage equal to or higher than 36 kV and that the access contract with the distributor or transporter has not yet been formalised.

For these purposes, access and connection permits for this type of facility are subject to article 23-bis of Royal Decree 1183/2020, of 29 December, on access and connection to electricity transmission and distribution networks ("**Royal Decree 1183/2020**"), which regulates the financial guarantees (either a bank guarantee or an insurance surety) for access and connection procedures for demand facilities (the "**Guarantee**").

The owners of these permits will have a period of six (6) months from the entry into force of Royal Decree-Law 8/2023 to file the Guarantee to the competent body, a period that ends on **28 June 2024**, and an additional six-month period to send the receipt accrediting the correct deposit issued by the administration to the network operator where the permit was obtained.

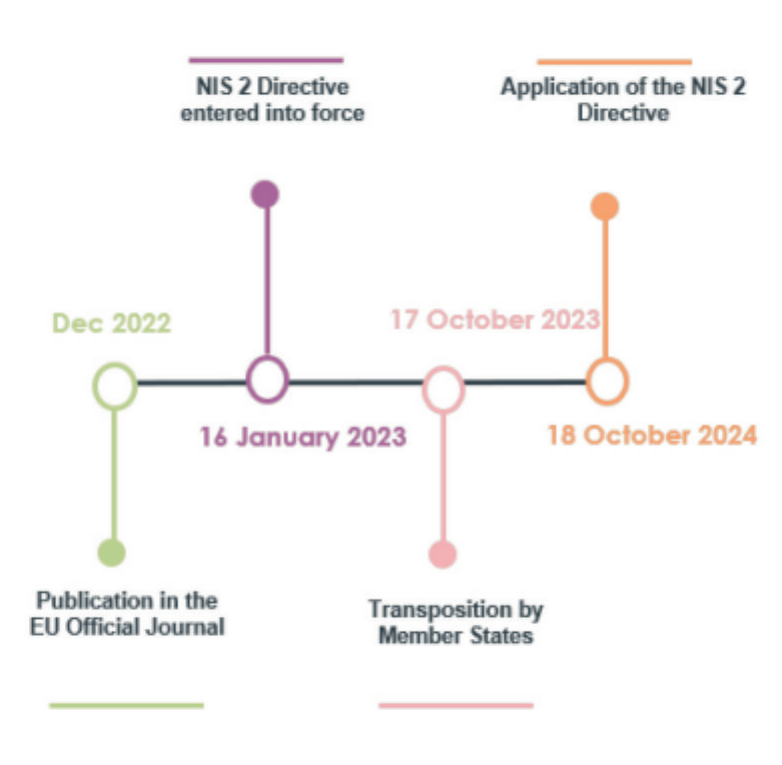
The amount guaranteed will depend on the power obtained in the permit since, in application of Royal Decree 1183/2020, the guarantee will be for an amount to **40 €/kV requested**.

The processing of the guarantees will have to follow the procedure established by the autonomous community where the installation is located. If they are in a territory that affects more than one autonomous community, they shall be deposited in the General Depository.

For more information, please contact Conchita Sainz and Coral Yáñez, who will be able to assist you on any queries or legal needs you may have on this new regulation regarding the Spanish market.

Data centres and cybersecurity – what to look at from an EU, UK and a Saudi Arabian perspective?

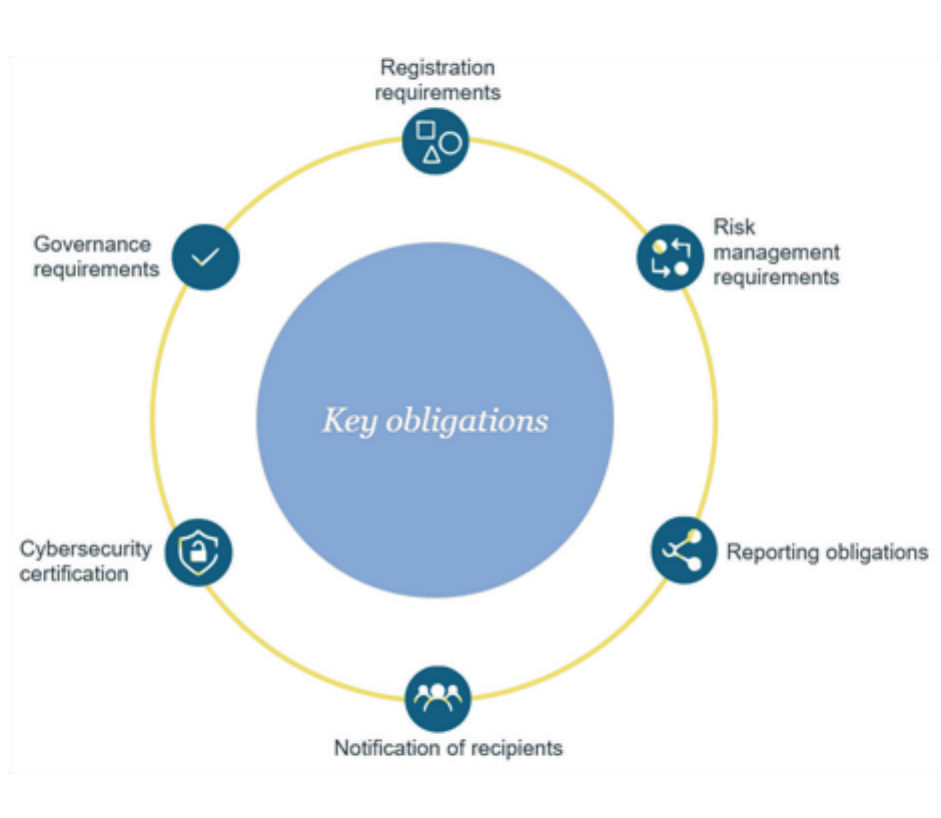
With the increasing focus on data security and network resilience, data centre operators need to be aware of and ready to comply with new strengthened cybersecurity obligations. We are witnessing a trend of increasing regulation in this area, with EU Member States now working on the transposition of the NIS2 Directive into their local laws (see our NIS2 Directive Implementation Tracker). The updated EU cybersecurity regime will apply from 18 October 2024 and has a direct impact on data centres. We a brief overview of the key elements and how to prepare for it. We also cover developments in the UK and the Kingdom of Saudi Arabia.



EU – new strengthened cybersecurity regime under the NIS2 Directive and national implementation applies to data centres – what do you need to do?

The key elements of the NIS2 regime (which strengthens and replaces the existing regime) are as follows:

- **Registration requirements:** Data centre operators will need to submit certain information to the competent authorities in connection with their registration obligations.
- **Strengthened cybersecurity risk-management requirements:** companies will need to have certain measures in place (e.g., measures regarding incident handling, business continuity, supply chain security, human resources security, access control policies and asset management) to manage the risks to the security of the network and information systems.
- **More detailed reporting obligations:** Incident reporting obligations to competent authorities and operators may also need to notify customers in certain cases.
- **Cybersecurity certification:** For the purposes of demonstrating compliance with cybersecurity risk-management measures, Member States may require data centre operators to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes.
- **Explicit governance requirements:** Senior management boards and committees will be required to approve and oversee the implementation of the cybersecurity risk-management measures. In addition, the members of company management bodies will be required to follow training and shall encourage entities to offer similar training to their employees on a regular basis.
- **Accountability of top management, supervision and enforcement:** The regime also introduces accountability and liability of top management for the non-compliance with cybersecurity obligations, more stringent supervisory measures for national authorities as well as stricter enforcement requirements and aims to harmonize sanctions regimes across Member States.
- **Administrative fines:** fines of a maximum of at least 10 000 000 EUR or of a maximum of at least 2% (of the total worldwide annual turnover in the preceding financial year can be imposed for non-compliance, whichever is higher).



What should data centre operators do now

- Carry out a scoping exercise to determine the applicability of the regime to your organization;
- Track and analyse the local NIS2 implementation in the countries of interest;
- Review current processes and procedures to assess what changes need to be made to align with the new requirements;
- Update incident response plans and processes, including those aimed at compliance with other laws, such as the GDPR, data breach reporting and telecoms reporting requirements;
- Draft a practical compliance plan with specific target dates;
- Review and update your contract with your service providers and suppliers;
- If you deal with customers operating in a financial sector, there may be additional requirements to consider, for example the application of the Digital Operational Resilience Act which addresses cybersecurity risks in the financial sector and impact ICT third party suppliers;
- Ensure that regulatory efforts in related areas (IT contracts, privacy, sector specific laws) are consistent.

UK - What are the key obligations under the UK cybersecurity regime?

Given Brexit, the UK is not required to implement the new NIS2 Directive and instead the old NIS regime as currently implemented in the UK under the Network and Information Systems Regulations 2018 remains in place.

This applies to:

- Operators of essential services
  - this relates to providers of services that are essential for the maintenance of critical societal or economic activities (e.g. water, energy, transport, health and digital infrastructure); and
- Relevant digital service providers – this covers providers of online search engines, online marketplaces, and cloud computing services – it does not directly apply to data centre operator unless they provide cloud computing services which may include cloud hosting services (if offered by data centre operators).

Notwithstanding this, the UK is proposing to expand the scope of this cybersecurity regime to cover managed service providers (noting that telecoms services will remain subject to the separate telecoms security regime in the UK). However, the changes have not been adopted yet and we are awaiting implementing legislation.

To the extent that data centre operators are providing services that are captured by the NIS regime (noting that cloud hosting services may be of particular relevance to data centre operators), it may be necessary to consider these cybersecurity requirements in the UK. There are no current plans to impose direct obligations on data centre operators unlike NIS2 in the EU.

Further, unlike the EU where telecoms security will fall under the scope of the NIS regime, telecoms services in the UK will remain subject to separate telecoms security requirements. The UK has recently implemented a new strengthened telecoms security framework which may be either directly relevant to data centre service operators if they also provide telecoms services or indirectly relevant where managed services are being provided to telecoms providers operating in the UK (i.e these providers may expect their data centre providers to have relevant safeguards, measures, procedures and processes in place as well as seeking to flow down obligations into relevant contracts so as to mitigate security risks as well as require them to complete supplier risk assessments).

KSA - What are the key cybersecurity obligations for data centres in the Kingdom of Saudi Arabia?

While data centre specific regulation was issued by the Communications, Space and Technology Commission (CST) in August 2023, including specific requirements for Data Center Service Providers to address physical security, they made no reference logical security. However, there is a significant weight of existing cybersecurity specific provision in the Kingdom.

In June 2020, the Communications & Information Technology Commission (CITC) issued the Cybersecurity Regulatory Framework for Service Providers in the Information and Communication Technology Sector (the "CRF"). The CRF provides a comprehensive set of cybersecurity requirements to be implemented by Service Providers in the ICT sector. The CRF distinguishes between Service Providers who are classified as Critical National Infrastructure (CNI) who must comply with the Essential Cybersecurity Controls (EEC) issued by the National Cybersecurity Authority (NCA) and those Service Providers who are not so classified who must comply with the CRF.

The CRF set out very detailed controls and requirements touching on Governance, Asset Management, Cybersecurity Risk Management, Logical Security, Physical Security and Third Party Security.

The EEC sets minimum cybersecurity requirements with the presentation of 114 cybersecurity controls for national organizations that are within the EEC scope – government organizations and their companies and private sector organizations owning, operating or hosting Critical National Infrastructures. Critical national infrastructure is defined as "infrastructure whose loss or susceptibility to security violations may result in significant negative impact on the availability, integration or delivery of basic services or may have a significant impact on national security, national defence, the KSA economy or KSA national capabilities".

The EEC are supported by the Critical Systems Cybersecurity Controls (CSCC) which focus on network segmentation, intrusion detection and the monitoring of critical systems. The CSCC applies to organizations operating critical systems and focuses on systems or networks whose failure, unauthorized change to their operation, unauthorized access to them, or to the data stored or processed by them may result in negative impact on the organization's businesses and services availability, or cause negative economic, financial, security or social impacts on the national level. The criteria identified in the CSCC for identifying critical systems are when a failure of that system has a negative impact on national security; a negative impact on the Kingdom's reputation and public image; a significant financial losses (more than 0.01% of GDP); a negative impact on the services provided to a large number of users (i.e., more than 5% of the population); a loss of lives; an unauthorized disclosure of data that is classified as Top Secret or Secret; or a negative impact on the operations of one or more vital sector.

The Cloud Cybersecurity Controls (CCC) were implemented to secure cloud-based data and applications and are a set of controls addressing data encryption, identity and access management and compliance monitoring.

The Data Cybersecurity Controls include the encryption of sensitive data, access controls, data retention and the requirement for data audits.

Also of significant relevance is the Kingdom's Personal Data Protection Law (PDPL), which came into force on 14 September 2023 to regulate the use of personal data in KSA giving a year within which to achieve compliance. Accordingly, note in particular that full enforceability begins on 14 September 2024.

While this paper is not the place for a detailed explanation of the PDPL, is it worth identifying that it includes the requirement of the adoption of security measures, including the regular assessment of security controls; identifying and addressing vulnerabilities; assessing system security through penetration testing; continuous security monitoring; and third party risk management.

For more information, please contact Anthony Rosen, Simon Shooter, Dr. Natallia Karniyevich and Hayley Blyth.

Colocation – lease or licence?

One of the oldest questions when looking at the occupation of property is whether an agreement between two parties constitutes a lease or a licence to occupy.

What is the difference? A licence is a personal permission to occupy property while a lease constitutes a legal estate and can give the occupier significantly enhanced rights to remain in occupation and/or renew at the end of the contractual term.

This question arises when looking at colocation agreements in relation to data centres.

If one were ever to find oneself in Court faced with the question of whether the property owner and the occupier have created a lease or a licence the Court would look at the substance of the agreement rather than what the agreement calls itself.

There are certain indicators that a Court will hold as pointing towards the agreement having created a lease, the most important of which is whether the agreement has given the occupier exclusive possession. What that means is whether the agreement provides for the occupier to be able to exclude third parties (including the owner apart from specific rights of entry it has reserved) from the premises it has taken. Other lease indicators include the reservation of a rent and the grant of rights for a fixed period.

In a data centre context one will typically find two scenarios. Firstly, there is the installation of servers in a shared room controlled by the data centre provider and secondly, there is the grant of rights to use a separate private cage or room.

Where there is a room shared by various entities, an occupier's colocation agreement is likely to create a licence. The data centre owner will control and operate the room and there will be no question of any of the users having exclusive possession.

However, where the occupier takes its own cage or room the position could well be different. If the occupier is granted rights to exclude third parties from the space it has taken then there is a risk that, whatever the colocation agreement may call itself, it in fact creates a lease.

The potential issue with a lease is that it may then have security of tenure under the Landlord & Tenant Act 1954 and this, in theory at least, will mean that it is more difficult for the owner to terminate the agreement at the end of the agreed term and will give the occupier statutory rights of renewal on the same terms and at a "market" rent.

Frequently people seek to avoid this outcome by including provisions in documentation aimed at avoiding any suggestion that what is being created is a lease. These will typically include provisions stating that the agreement constitutes a licence not a lease, a statement that the owner retains possession and control of the property being licensed, a statement that the licence being granted is personal, and a provision that the owner can move the occupier to alternative space on notice.

It isn't clear whether this approach will always work in a data centre context. It is established law that the fact that an agreement calls itself a licence won't make it a licence (although there has been some judicial comment in more recent years potentially lending more weight to arguments that it does). As for the owner retaining possession and control, typically a party taking its own room or cage will want to ensure that it has control over that area itself. As for the agreement being personal, whilst a true occupational licence will be personal, there are many leases that prohibit assignment. Finally, what is the position when an occupier signs up an agreement providing for relocation in a data centre where relocation is not a practical possibility?

Is any of this a concern in practical terms? Providers in general appear to take the view that, even where exclusive possession is being granted, it is easier just to have people signing up on standard colocation agreements. Furthermore, given the particular nature of the data centre market, one rarely hears concerns voiced regarding the potential risk of renewal on the same terms and at a rent potentially determined by the Court. However, providers would be advised to bear the legal possibilities in mind.

For more information, please contact Andrew Stobbart.

Early contractor involvement (ECI) to de-risk the construction of data centres

Generally, when considering what the definition of a successful project (such as a data centre) is, it is a project that is completed:

- On time
- Within budget
- In line with the specifications
- Without disputes

Traditionally the focus with the contractual set up of contracts dealing with a construction project is to have three types of parties involved: the employer, the designer/engineer and the contractor. Each party has its own role during a construction project, and does not venture into the scope of the other two parties. In respect of construction contracts, these tend to be focused on dividing and allocating tasks and risks. Whilst they work together on a project, each party stands on their own if there is an issue. This has been a very successful model, especially for projects with a relatively low risk profile and/or sufficient time & resources to identify and manage risks during the preparation phase.

However, projects are increasingly turning complex and when, as for data centre projects, these involve the complex interrelationships between different components, it is easy to see that this model might create problems. A large number of data centre projects are still one-off projects, with project specific challenges related to for instance soil conditions, use of technological components, permitting, and ever changing requirements from stakeholders (such as end-users, local authorities and local interests groups). Other sources of challenges may be from increasingly complex circumstances set by for instance the supply chain, local utility providers/grid connectors and investors/financiers.

One way to decrease the risk profile, or in any case a contractor's assessment thereof, is to be involved early on and have sufficient opportunity to assess, mitigate and price risks. Such early involvement is also referred to as early contractor involvement (ECI). ECI is an approach we have been adopting in a range of data centre projects, through ECI contracts which are sometimes also referred to as preliminary or pre- construction services agreements (PCSA).

Applying early contractor involvement (ECI) during the preparation stage amongst others:

- Improves the knowledge of contractors & suppliers and allows them to do research before starting construction, therefore improving the chance of success.
- Can allow for further optimizations (i.e. from price, safety, sustainability, planning or technical perspectives).
- Can ensure that the price finally agreed upon with the contractors & suppliers is a good reflection of the actual costs, rather than a 'guesstimate'.
- Can allow the employer to weed out any contractors & suppliers who are not up for the job before having them starting the works (should they be uncooperative, not-proactive, unknowledgeable etc.).

To further boost the usage of ECI, our partner Andrea Chao's role as chair of Task Group 17 of FIDIC has co-initiated & co-developed the model ECI contract DG2020. This model seeks to incorporate both a legal and project management approach to this form of contract, and has specific attention for the type of collaboration and behaviour expected. Currently, this model is being updated in order to allow the incorporation of experiences from the procurement of hundreds of projects with a combined value of Billions of Euros. A new version is scheduled to be launched early 2025. This model can be found through this link: Microsoft Word - Model Agreement Early Contractor Involvement

Bird & Bird have extensive experience with such contracts for the purpose of development of data centres, ranging from procurement and drafting up to contract management. Please do reach out to us if you want to explore how this approach could support the delivery of your project.

For more information, please contact Andrea Chao and Marco Nicolai.

Utilizing collaborative contracts to increase a successful delivery of data centres

In our **previous article** we touched upon a range of challenges we are currently seeing on the development of data centres. We also touched upon how Early Contractor Involvement (ECI) can be adopted to address such challenges. There are also other legal tools that can be utilized. In this article we will touch upon the legal tool referred to as *'collaborative contracting'*.

The aforementioned challenges are all characterized by the fact that neither the employer nor the contractor can successfully tackle these without the involvement of the other party, and that the solution may only be identified at a far advanced design phase. Adding to the complexity is that nowadays it is not uncommon with such assets to work with a multi-contractor approach. Rather than having one single contractor acting as general contractor and being the main point of contact, the employer increasingly choses a multi contractor approach. This includes Owner Furnished Contractor Installed (OFCI), but may also be the result of sheer pressure by current market circumstances.

Consequently, for construction projects facing one or more of the challenges mentioned above, traditional contracts might not be the best route to help deliver a successful project. This is giving rise to the development of a range of collaborative contracts: contracts that seek to improve the engagement, active communication and collaboration between employer and contractor.

Collaborative contracts, sometimes also referred to as relational contracts, often include one or more of the following elements:

- Early contractor involvement (being the topic of the previous article).
- Applying a joint risk and decision-making process throughout the project.
- Applying collaborative contracting throughout the project.
- A collaborative contractual model adopts the view that the contract not only needs to describe the goal but also needs to describe how that goal is to be achieved, thereby giving the developer a more active role. This is not only a legal tool but also a project management tool, which helps deal with surprises during a construction project as effectively as possible.
- It ensures that parties continuously communicate, align, are aware of the process, are on the lookout for issues & solutions (even if these do not relate to their own work package) and hold each other accountable (especially in a non-legal manner). Therefore, it is geared towards mitigating (interface) risks.
- The employer, and where needed: also other stakeholders, to have an active role.
- It ensures involvement of the chain of suppliers & contractors (as these are often the answer to problems, and sometimes also the cause thereof).

Bird & Bird have extensive experience with such contracts, and in drafting new model contracts. Bird & Bird are contributing to the development of an international standard collaborative contract through our partner Andrea Chao's role as chair of Task Group 17 of FIDIC, which is tasked with the development of such contracts for the FIDIC Contract Suite. This contract is expected to be launched end of 2024/early 2025. Please do reach out to us if you want to explore how this approach could support the delivery of your project.

For more information, please contact Andrea Chao.

Events

5 - 6 June

Datacloud Global Congress 2024, Cannes

Bird & Bird is proud to be sponsoring Datacloud Global Congress this year in Cannes and we would love to see you there.

Come and listen to:

- Simon Shooter speak on the panel "Are we taking Cyber Security seriously?" on Wednesday 5 June at 1:30pm in the Innovation Theatre (Expo Floor) and;
- Roger van Buuren speak on the panel "How are we financing our data centres?" on Thursday 6 June at 11:10am at Datacloud Engage (Press Room – Level 2).

Do also join us for a cocktail reception on the Windrush II, click here to register. Marco Nicolai, Sibylle Weiler, Dr. Dirk Barcaba, Boris Martor, Sophie Phillips, and Roger van Buuren from our Data Centre team will also be attending.

We look forward to connecting and discussing all things data centres!

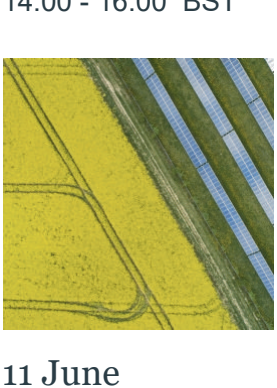
5 June

Online

14:00 - 16:00 BST

How to balance fundamental rights and data protection?

Join our LinkedIn Live event on Wednesday 5 June 2024, where our leading panel of privacy experts will discuss the opinion's compliance with EU law and CJEU decisions as well as its potential impact of this opinion on EU businesses, data driven business models and the EU's data strategy as well the EU digital economy.



11 June

In-person

13:30 - 20:30 BST

Energy Futures Conference

We are delighted to invite you to our second annual Bird & Bird Energy Futures Conference where we will focus on the key role of innovation in the energy sector, including the opportunities and challenges to be overcome to get keep the sector moving forward at pace. Our expert speakers will share insights, discuss trends, and explore the legal environment which can enable the latest innovative breakthroughs in clean energy.

20 June

Online

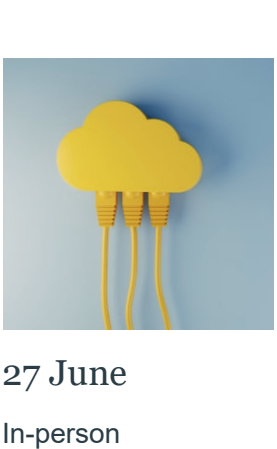
08:30 - 09:30 PDT

Decoding the Data Act: deep dive into cloud switching and interoperability requirements

In this webinar, our Bird & Bird experts will cover the following topics:

- State of play of the cloud market and switching between providers
- Data portability requirements pursuant to the Data Act
- Elements for contractual reviews and compliance
- Interoperability for data processing services
- Common specifications and harmonised standards

Our experts will provide you with a practical checklist to assess what businesses need to prepare for prior to the entry into force of the Data Act.



27 June

In-person

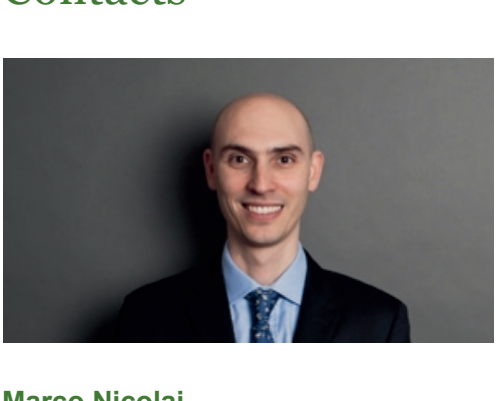
13:00 - 17:30 BST

Data Protection in 2024: A review of the year so far and a look ahead to 2025

We are thrilled to be running our annual data protection update event at our London office on 27 June 2024.

Our experts will be providing an overview of key developments and points to watch in the UK & EU. AI is everywhere - including at our update - where we will delve into the AI Act and AI governance. We'll also be exploring key updates on ad-tech developments.

Contacts



Marco Nicolai
Partner, UK
+447725 372 522
Marco.Nicolai@twobirds.com

Sophie Phillips
Senior Associate, UK
+447840 041 211
Sophie.Phillips@twobirds.com

Follow us on LinkedIn & X