Hogan Lovells

Welcome to the world of data centres

Investments in a new asset class: Success factors and pitfalls

2019

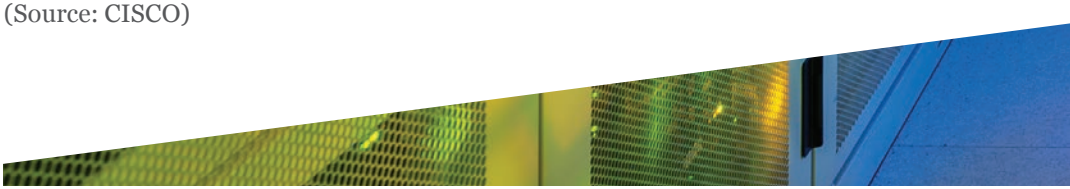
Introduction

Hogan Lovells is your first port of call and the leading legal provider in relation to successful realization and investments in data centres in Germany and Europe.

Our dedicated data centre team comprises lawyers with an in-depth understanding of the data centre industry and its characteristics. When providing you with closely coordinated one-stop advice, we bring together our knowledge carriers from various legal disciplines including Real Estate, Infrastructure, Energy, Resources & Projects, Intellectual Property, Project M&A, Data Security, Dispute Resolution, Corporate, Commercial, Project Finance, Employment Law and Tax Law. This approach adopted by our integrated industry sector team ensures that you receive consistent, industry specific and solution oriented advice which focuses on what you really need.

This brochure summarizes key legal aspects to be considered when buying, selling, financing and/or constructing a data centre, including data protection, digitalization and cyber security.

In the last 3 years the datacentre workload has grown on average by more than 20% worldwide. This development will continue in the coming years until at least 2021. (Source: CISCO)



What we offer:
Many years of experience, a deep understanding of your industry, and a solution oriented focus.


1X
2X

Welcome to the world of data centres

Lease or build a data centre?

When a company is growing and wants to out-source servers and IT equipment, it must de-cide on the best way to do this. Such a decision can be crucial if the business is expanding rapidly and therefore urgently requires additional space for servers and IT equipment. The choice it faces is whether to lease data centre space (by a colocation or warehouse solution, which we will refer to as "leasing" or a "leasing solution") or whether to build its own data centre.

The obvious advantages of building over leas-ing are that

- the company has maximum control over the IT equipment and anything related to it;
- there is no risk of "losing the lease", and
- any unused space can be leased out to other companies, thus reducing electricity, cooling and security infrastructure costs.

On the other hand, the main disadvantages of building are upfront costs which can add up quickly if not calculated thoroughly. The costs of building and maintaining a data centre should not be underestimated and may be a crucial factor in the decision making process. When evaluating the costs involved, the focus is mainly on power, staffing and IT infrastructure. However, real estate related costs are often not taken into account sufficiently or at all. These include architect, planning and design costs, building costs including costs for permits, such as building permits, costs for fire suppression and detection systems, notary costs, costs of registrations, etc. Nor should companies underestimate the various risks related to power and cooling infrastructure, hardware and software, technological development, uncertainty surrounding future business strategy and potential space problems, i.e. if the space later proves to be too small or too big. Moreover, companies should be aware of the large number of building regulations to be met, for example in the area of fire safety which may be very strict in some jurisdictions. On balance, leasing is likely to be a better solution for many companies because it allows risks to be confined and gives companies the flexibility to adapt their space needs to their business needs.

Data centre leasing strategies – the various types of contract structures

The most common types of leasing structures for data centres are:

- Wholesale data centre and colocation solutions
- Server hosting – managed hosting

Balancing the need for control with the desire to cut costs

Ultimately, the decision between a whole sale/colocation structure and a purely managed hosting structure is one of balancing the need to control the servers and IT equipment with the desire to achieve the

best possible cost savings by entering into a data centre lease. Important topics which need to be addressed before taking such a decision include:

- how much control is necessary with respect to operation of IT equipment and the premises in which the IT equipment is stored;
- whether the tenant is prepared and willing to accept (high) capital expenditures for repairing and updating IT equipment; and
- whether the tenant is prepared to employ and pay for the necessary personnel to operate and maintain the IT equipment.

When taking this decision, the tenant should not only consider its present situation and its needs as a business, but also bear in mind its future strategies and plans in order to find the best solution. Overall, the wholesale/ colocation solution or a hybrid solution might be the right choice for many bigger companies, whereas the managed hosting solution could be the ideal solution for smaller firms.

What a data centre lease should cover

First and foremost, it is vital to clarify the legal relationship between the data centre provider/landlord and the occupier/ customer. Depending on the actual use and allocation of rights and obligations, a lease agreement (triple net or double net), a service agreement or an agreement with lease and service elements are possible options. In the majority of cases, the parties will sign a lease agreement which also includes elements of a service agreement.

As the lease agreement is the main legal document which governs the relationship between the parties, particular care should be taken when negotiating "Provider Must Haves" on the one hand, and "Customer Must Haves" on the other. Key topics to be considered in lease agreements include:

Lease term and renewals

Would the company prefer a long-term or shortterm lease taking into consideration that the initial term is often 15 to 20 years? In addition, the number of renewal periods and any pre emptive rights of the tenant should be taken into account.

Rent payment

Another important point is how the rent will be paid. The basic rent is usually based either on square meters or on power availability.

Space, permitted uses and equipment

The leased space might not be enough for all the equipment and infrastructure that the tenant requires. It is therefore advisable to stipulate in the lease agreement whether the tenant is allowed to use additional space, e.g. on the roof for antennas, shaft space within the building or special support areas for the placement of generators.

Set-up, alterations, maintenance, repair and replacement

Depending on who owns and who will be obliged to maintain the facility infrastructure, specific provisions must be incorporated into the lease agreement regarding alterations, maintenance, repair and replacement. The tenant and/or landlord might be required to comply with certain standards and/or maintenance schedules. Provisions on services relating to data centre equipment, heating, ventilation and infrastructure should also be included.

Power supply, cooling, humidity, connectivity and data capacity

Power supply, cooling, humidity, connectivity and data capacity are the core topics of a data centre lease. Provisions covering these areas must therefore be included in the agreement. Specifically, the following topics should be dis-cussed and agreed: power requirements, cost of power and uninterrupted power supply as well as redundant fibre access, multiple carriers and sufficient data capacity.

Service level agreements

The parties should also consider including service levels and reasonable support provisions. Moreover, the agreement should describe what happens if service levels are not met. For the customer, it might be desirable to include a termination right for continued breach of guaranteed service levels.

Liability, indemnification, data protection and security

A limitation of liability might be beneficial for both parties. The agreement should also include provisions regarding data protection, security (e.g. access to the building) and compliance with laws.

In addition to the key topics mentioned above, it might be advisable to incorporate other provisions, depending on individual circumstances.

Avoiding pitfalls in construction contracts

Unlike brownfield projects/transactions, developing greenfield data centre projects are challenging and come with various risks. The developer needs to decide on the right approach for such a development: Delivering the project with various (multi-lot) contractors and a potential designer/or engineer or choosing an turnkey approach whereby an EPC-Contractor delivers the whole projects and agrees to engineer, procure and construct the datacentre. While the first option may deliver a more cost-efficient solution, a turnkey EPC Contractor undertakes the full completion, turnkey and interface risk of such a highly complex project. One of the most obvious benefits of entering into such a contract is having one single point of contact and responsibility for the project, thereby avoiding having to manage various role-players that would otherwise have to be involved in the construction and setting up of such a project.

While it is, of course, commonplace for an EPC Contractor to engage various subcontractors to provide certain services or works, the EPC Contractor remains the single point that is directly responsible for ultimately delivering a project ready for operation. This means for the Employer in an EPC project that the added risk of liaising with various parties and allocating various risks is avoided.

Parties need to face reality in terms of construction of a data centre. According to KPMG International's 2015 Global Construction Project Owner's Survey,

- Major complex EPC projects fail more often than they succeed, resulting in disputes;
- 71% of owners in the energy and natural resources sector reported unsatisfactory underperforming projects; and
- 69% of all projects between 2012 and 2015 were reported to be more than 10% over budget

Having this in mind, a clear contractual framework including a fully functional and efficient claims and risk management can assist in avoiding pitfalls as well as significant delays and cost overruns.

Getting your contracts right

Service level agreements with respect to data centre leases

A service level agreement is the main contract that defines the parties' rights and obligations under a data centre lease.

Before signing such contracts, the parties should assess the scope of services that the data centre landlord will perform under a service level agreement. These services could range from entire business processes or merely IT processes, through to the exclusive provision of IT infrastructure within the data centre.

More elaborate service level agreements may also stipulate the provision of certain types of software (applications) by the potential financiers (application service providing, "**ASP**").

Such an assessment is a key consideration for the validity of any service level agreement. The scope of the data centre lease and the rights and obligations of each party may vary according to what was agreed upon between the parties. In any case, it sets the standard for the evaluation of the agreement with regard to the law on General Terms and Conditions.

However, both IT and data centre services are prone to faults, require maintenance or updates and may be subject to cyber attacks. All these and other adverse effects may lead to downtimes and impact on the availability of the data centre. With regard to the strict applicability of the law on General Terms and Conditions, the parties are advised to ensure that the availability of the data centre is laid down in the agreement. Conversely, the landlord faces the risk of having to guarantee the permanent availability of the data centre.

The parties should not include a disclaimer regarding warranty claims. The statutory warranty obligations of the landlord or the contractor cannot be excluded within the General Terms and Conditions in many jurisdictions for instance.

Finally, the parties should assess the validity of any limitation of liability clause regarding strict liability on a case by case basis. However, the limitation of the landlord's liability should always take into account the risk of cyber attacks and appropriate preventive measures.

Getting the operation structure right

When it comes to the operation and maintenance of data centres, it is all about availability, reliability and stability of the services. Just recently, some parts of the German World Wide Web were interrupted for several hours due to a downtime of an internet hub in Frankfurt as a result of an energy breakdown in a Frankfurt date centre compared with a crash of the energy redundancies in this data centre. Even short outages of the energy supply, the cooling of the racks or the humidity control in the data centre may cause enormous downtime costs and high damage. Thus,

uninterrupted availability and fast troubleshooting services are required and should be secured at any time.

A key instrument for securing such availability and avoiding potential losses can be seen in liquidated damages. Liquidated damages are designed to meet the legal requirements in the relevant jurisdictions and may help to keep the pressure on the operator in order to secure quick troubleshooting and sufficient redundancies of the contractor. In some jurisdictions (such as Germany), a well thought-through drafting of contractual predefined liquidated damages is essential to avoid unenforceable provisions.

In order to achieve this, the party engaging an operator should extensively investigate and consider in detail all possible scenarios which may lead to interruptions in the services. Especially the core services (e.g. power supply, cooling, humidity control, security) should then be discussed with a view to defining contractual service levels, percentages of guaranteed availability and pre-agreed reaction and trouble shooting times. In particular, the contractual service levels should ensure that the required times for (successful) troubleshooting and the points of measurement of the availability are exactly defined. The better the parties describe such obligations and service levels in the contracts, the better they may be able to link these times and percentages to an escalating mechanism of liquidated damages covering the employer's potential damage in a realistic manner.

Data centre M&A and Financing

Share vs. asset deal

In an acquisition scenario it should be decided as early as possible whether the transaction will take the form of a "share deal" or an "asset deal".

Under a **share deal**, all or part of the shares in a business are transferred to the purchaser. If, for instance, a project company or holding company has been set up as a limited liability company, the purchaser – upon completion of the purchase – becomes a shareholder of that company.

In contrast, under an **asset deal**, the seller only disposes of and transfers individual assets (and liabilities) under an asset purchase agreement (APA). On the basis of the principle of legal certainty in some jurisdictions, the transferred assets and liabilities must be clearly defined in the APA together with any required particular kind of transfer method to the purchaser. Therefore, an asset deal initially also involves increased costs and effort on the part of the seller and the purchaser to establish and agree on the "object of the purchase" and the contractual documentation (i.e. the APA). However, the advantage of an asset deal lies in the possibility to select individual assets and liabilities for transfer. Any ancillary contracts (incl. rights and obligations e.g. power purchase agreements, commercial agreements such as lease agreements for the provision of data centre services) will have to be transferred to the purchaser separately by way of novation. In particular, it should be noted here that – in contrast to a share deal – both the sale and transfer of the contractual relationships re-quires the consent of the contractual partner.

In the course of a share deal, the purchaser will acquire a certain percentage of the shares in a target company from the shareholders of that company, including any and all of the target company's contractual relationships, receivables and liabilities on the basis of a share purchase agreement (SPA). Unless dedicated "change-of-control" provisions apply, no consent from the other contractual parties is required, as it is only the shareholder of the counterparty (the target company) that changes, not the counterparty itself. Potential risks, in particular on the investor/purchaser side, arise not only from the acquired assets themselves, but also potentially from the underlying entity that actually owns the assets and whose shares have now been acquired by an investor/ purchaser. Consequently, since under a share deal the transaction does not affect any existing contracts – claims by employees, third parties as well as long term contractual relationships potentially unknown to the purchaser will be assumed – this risk should be mitigated by way of in-depth due diligence as well as by imposing an appropriate guarantee and liability regime on the seller in the SPA.

Nonetheless, transactions involving data centres are typically implemented as share deals, in particular because they allow a clean exit for the seller and a comprehensive acquisition of rights and assets for the purchaser. However, asset deals may be preferable if the target company bears major liability risks (e.g. from other operations or from pending disputes with customers), or if the transaction takes place in the context of a crisis or insolvency proceedings of the target company (distressed M&A). In summary, the question of whether a share deal or an asset deal is preferable cannot be answered in general – the decision must be taken following an assessment of the interests of the respective party (seller or purchaser) and the specific transaction.

Due diligence – the best of both worlds

Our practical experience repeatedly confirms that due diligence in data centre M&A transactions significantly differs from due diligence in traditional M&A transactions. This aspect is frequently underestimated and often leads to risks not being identified and therefore not reflected in the underlying share (or asset) purchase agreement.

By nature, data centre acquisitions require a different approach to due diligence. While it

may be sufficient in "traditional" M&A to summarize the key provisions of the commercial agreements (such as termination and change of control) and to examine whether the agreements are legally binding, this is not enough when dealing with data centre projects. The traditional approach tacitly assumes a large number of commercial agreements and that these agreements are implemented according to their provisions, without any "problems" arising.

This approach is too simple for the data centre world. It tends to be the rule rather than the exception that for instance only a limited number of (long term) and commercially highly relevant lease agreements are in place – and the loss of just one of those agreements may jeopardize the buyer's assumptions in its financial model and accordingly the success of the entire transaction.

Therefore: heads up! We mitigate such transaction risks by conducting risk-based and tailored data centre due diligence that analyses the commercial agreements as part of a stress test and takes into account the specific characteristics of the respective data centre: we review in detail any lease agreements, power purchase agreements with a view to ensuring uninterrupted power supply and cooling of the facilities, as well as any other operation and maintenance agreements that are critical for the operation of the data centre. Ultimately, this means that our clients can be sure of correctly identifying the risks inherent in the often complex contractual documentation and of avoiding any unpleasant surprises later on – this is a significant success factor for any data centre transaction.

In this regard, we believe that a careful examination of the data centre specific agreements yields the best results if it is carried out by lawyers with appropriate drafting and negotiating experience. Only they are able to rapidly and reliably understand which scenarios will have which effect on the project agreements. Our experience of providing legal advice for data centre project developments means that we know what can go wrong and are thus able to identify typical risks.

As a result, our clients are aware not only of the current status of the agreements, but also of precisely what may lie ahead – and what does not.

Focus on cash flows – not on warranties

The approach to share (or asset) purchase agreements in a data centre transaction differs significantly from "traditional" M&A.

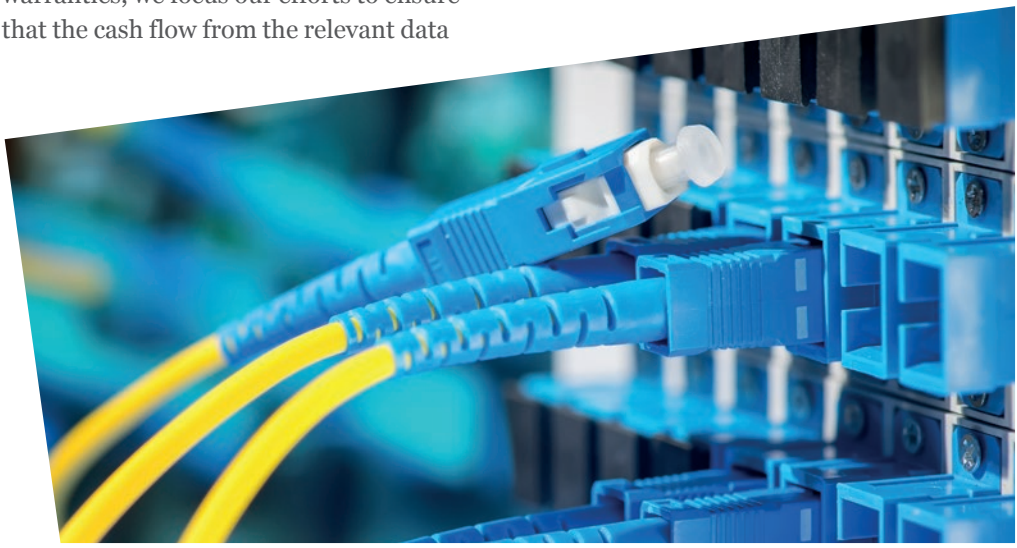
In contrast to traditional M&A transactions cash flow and profit are often not generated via the sale of goods and services to a market, but via a small number of key contracts – and sometimes only one. This makes investment attractive for long term strategic and financial investors, but also shows that the return is dependent on these contracts.

In addition, data centre deals often have a simpler asset structure than "normal" transactions. A lot of representations and warranties which are market standard in traditional M&A are not required in data centre M&A or, even worse, give a false sense of security. It would be fatal if a buyer of a data centre that generates profits under one or two long term lease agreements only relied on an extensive set of representations and warranties and did not take into account that such representations and warranties are usually time barred for 12 to 18 months after closing, often leaving the major part of the contract term unprotected.

As a consequence we have adopted our approach to the "data centre SPA". Instead of having lengthy and costly discussions on partially meaningless representations and warranties, we focus our efforts to ensure that the cash flow from the relevant data centre is protected in the SPA, as this is the real asset which is bought in a data centre M&A transaction. This approach only requires a limited set of representations and warranties, but needs to ensure that if those turn out to be wrong, the entire loss in cash flow is compensated. By focusing the SPA discussions on the relevant issues, we are usually able to significantly reduce negotiation time and to ensure that the SPA is structured and easy to understand. This approach also frequently helps our buy side clients to strengthen their position in auction processes in the highly competitive and seller friendly data centre market.

Project finance vs. corporate finance

Data centres involve significant capital in-vestment. A data centre's operator may wish to finance either the development and



construction or the acquisition of a data centre with debt. Whilst it is possible to source funds with all the usual instruments of corporate finance, the revenue stream generated by operating a data centre can also be suitable for project finance. Project finance is typically described as the long term financing of infrastructure and energy projects held in a special purpose vehicle (SPV) with a non recourse or limited recourse financing structure. The key characteristic is that the project debt is exclusively repaid by the cash flow generated by the project. No other income is typically available and the providers of both types of debt must rely on the success of the project to generate sufficient and stable cash flows. The project's assets, rights and interests serve as collateral. Compared to project finance in other sectors, the financing of a data centre also includes elements of real estate finance:

Given that the owner of a date centre is normally also the owner of the land, one of the main security rights provided to the debt providers is a land charge in many jurisdictions.

It is also not uncommon to work with an OpCo/PropCo which is also an element known from real estate finance.

One of the core elements for successful financing is a well structured and realistic business case. The date centre operator must therefore have a clear picture of the investment costs, an appropriate contractual set up for the reliable and secure performance of the development and construction as well as of the long term operation of the data centre and the expected return. Securing a long term lease agreement with at least once anchor tenant which accounts for a substantial part of the business case is therefore key.

PropCo – OpCo structures with respect to data centre leases

Tax optimization helps: A PropCo-OpCo lease structure can be used e.g. to reduce exposure to German trade tax, a tax levied by German municipalities (around 15-16% in larger cities).

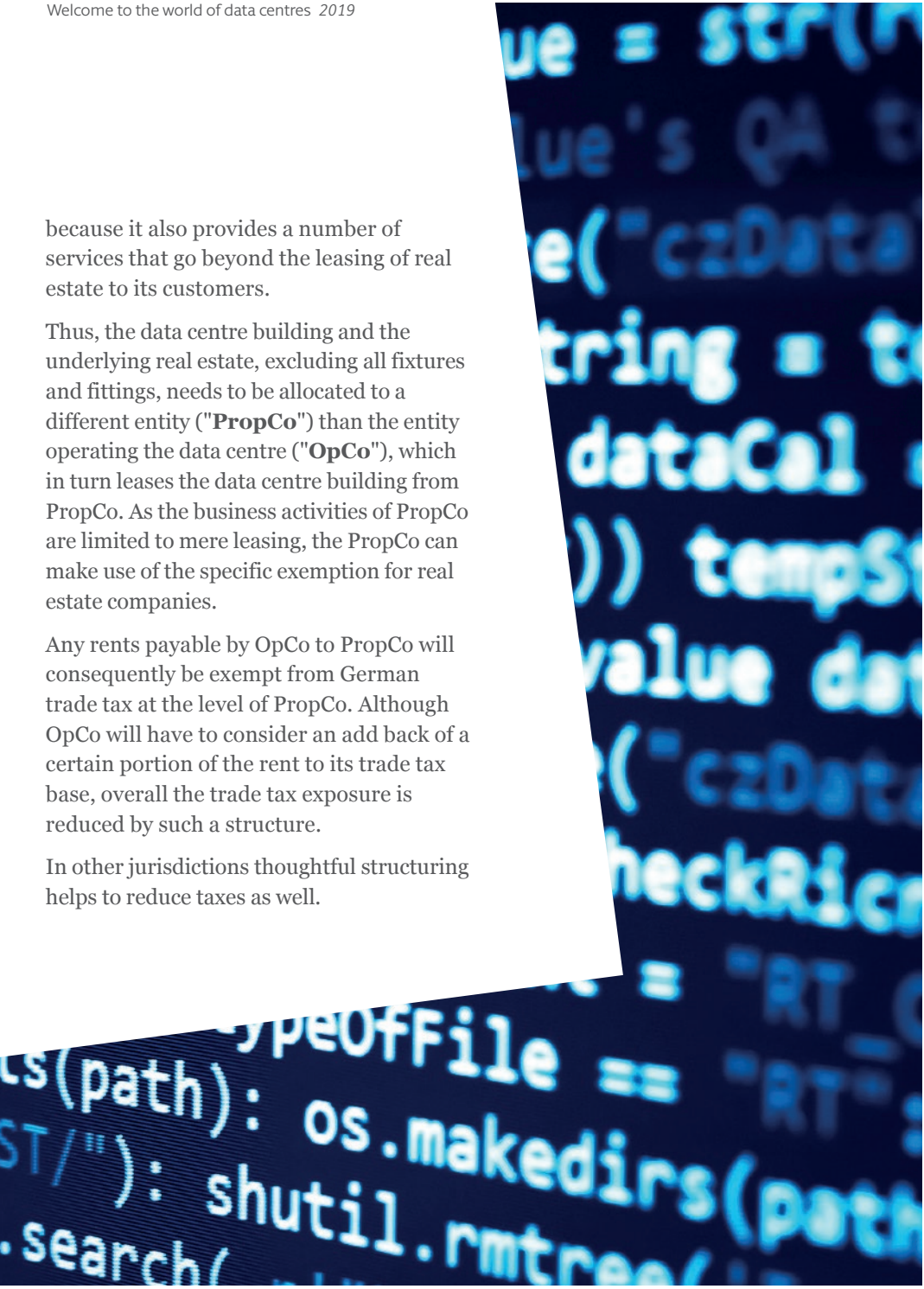
Real estate companies, i.e. companies engaged exclusively in the mere leasing and letting of their own real estate, are able to reduce their trade tax exposure to zero. A company owning and operating the data centre cannot apply this exemption

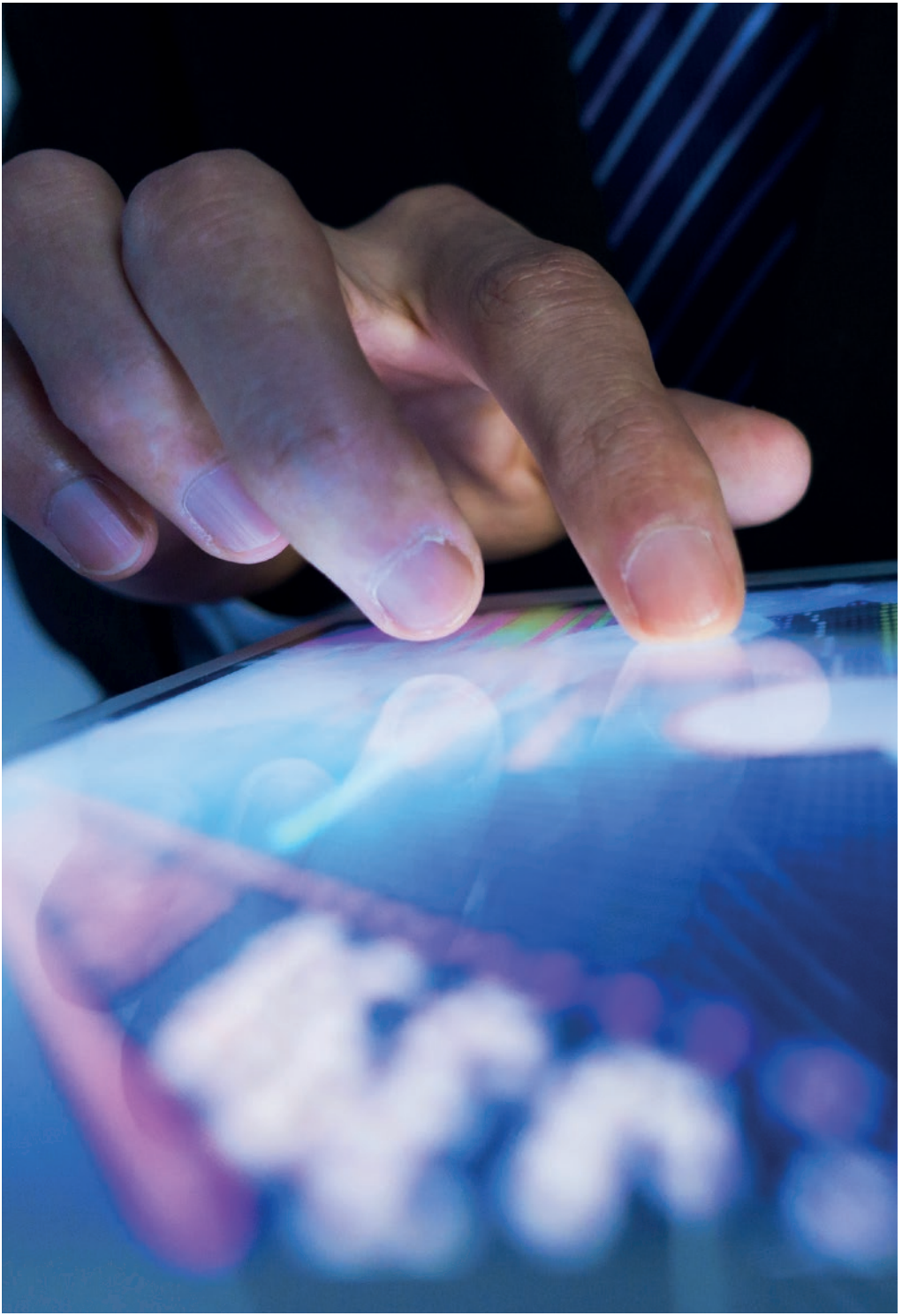
because it also provides a number of services that go beyond the leasing of real estate to its customers.

Thus, the data centre building and the underlying real estate, excluding all fixtures and fittings, needs to be allocated to a different entity ("**PropCo**") than the entity operating the data centre ("**OpCo**"), which in turn leases the data centre building from PropCo. As the business activities of PropCo are limited to mere leasing, the PropCo can make use of the specific exemption for real estate companies.

Any rents payable by OpCo to PropCo will consequently be exempt from German trade tax at the level of PropCo. Although OpCo will have to consider an add back of a certain portion of the rent to its trade tax base, overall the trade tax exposure is reduced by such a structure.

In other jurisdictions thoughtful structuring helps to reduce taxes as well.





Energy and efficiency

Energy: optimizing cost efficiency and minimizing risk

Every data centre operator will eventually have to address one considerable cost factor of any such operation: energy costs. Fortunately, operating a data centre offers numerous opportunities for energy cost optimization on both the operator and tenant side.

One of the goals for operators is probably to maximize their data centre's power usage efficiency ("**PUE**"). The PUE is the ratio of a centre's overall energy consumption versus the energy used by the IT installation. Ideally, the PUE equals 1. In this case, all energy consumed in the data centre is used to power the IT infrastructure and no additional energy is required for auxiliary equipment, i.e. for cooling or lighting.

Although a PUE of 1 is a theoretical value, there are several ways to get as close as possible to this figure. One of the most promising methods is to use a combined heat and power plant ("**CHP**"), which converts heat from the IT hardware into electrical energy and simultaneously provides cooling through absorption refrigeration.

On the tenant side, an increase in energy efficiency can be achieved particularly by maximizing the efficiency of the hardware in use. This includes efforts such as virtualization. Other, physical measures comprise the use of state of the art energy saving computing platforms. It should be noted, however, that in order to incentivize tenants to take such measures, it is essential to meter their individual power consumption. Additional incentives for tenants to reduce energy consumption may be contractually agreed.

Finally, it is possible to obtain long-term loans at favourable interest rates for measures to increase energy efficiency. With regard to the German market, for example, such loans are offered by the German bank *Kreditanstalt für Wiederaufbau* (KfW).

Disaggregated recursive data centre-in-a-box (dReDBox)

Besides energy costs, data centres are limited by the available space. Today, once the IT infrastructure is established, it is set in stone, and any changes can only be made with significant effort. So processing capacity, memory and other resources are allocated to one specific user. This means that connections, once established within the data centre ecosystem, will stay as they are even when these resources are not required by the user (server asaunit model). This leads to a significant waste of space, energy and computing capacity.

The European Union (EU) aims to tackle this static concept in order to create a socalled disaggregated recursive data centre in a box (dReDBox) as part of the Horizon 2020 pro-gram (H2020). The aim of this research project is the more flexible and on demand creation of interconnections within a data

centre ecosystem. Reacting to user demand and shifting resources where they are needed will unlock the full potential of the – currently unused – data centre infrastructure. As a result, efficiency gains are achieved while electric power consumption is reduced.

The dReDBox is based on pooling otherwise disaggregated IT resources. Pooling the IT infrastructure to match the needs of cloud users is intended to lead to improved utilization, scalability, reliability and power efficiency (pooled computer model). With regard to the generally limited space capacity of data centres, this will eventually enable the data centre operators to do more with their space while consuming less energy. Although this sounds utopian, three initial prototypes of the dReDBox have already been developed and are undergoing test operations to demonstrate the value and capacity of pooled data centre infrastructure with regard to cyber security, network analytics and telecoms.

Energy regulatory

Operators should carefully assess options for onsite power generation because, if structured appropriately, this could generate an additional income stream. Energy produced by solar panels and/or a CHP on-site and fed into the public power grid is very often subsidized and operators profit from comparably high feedin tariffs. Additionally, tax reductions may apply.

From a regulatory perspective, operators should ensure an adequately scaled grid connection for the data centre. In this regard, the relevant agreements with the grid operator – and if applicable with the land owner – need to be in place. As a stable and uninterrupted energy supply is paramount for the operation of a data centre, contractual regulations on down times of the grid connection for maintenance reasons should be reviewed carefully. Therefore it is important to be familiar with applicable regulatory and market standards.

Due to the importance of energy supply and cooling systems, data centre projects are in an excellent position to integrate onsite energy generation facilities such as solar panels or CHPs. If structured in compliance with the regulatory framework, the advantage of such onsite generation is that it allows operators to avoid some of the taxes and levies that typically increase energy costs. By using energy that has been generated onsite, operators may thus avoid paying grid usage fees, electricity tax and in certain cases even

further levies. Further more, operators should assess opportunities to benefit from government subsidy programs for investments in onsite renewable energy facilities or CHPs.

In order to assess the options for on-site energy generation, operators may consider entering into a so called energy contracting agree-ment with specialized service providers. The scope of such agreements varies from a mere assessment and planning exercise for a project to the complete financing, planning and operation of onsite energy generation facilities. When negotiating contracting agreements, it is vital to understand the applicable regulatory framework in order to identify potential pitfalls.

For green field projects, there are specific energy regulatory requirements resulting from European regulations. For example, land owners are obliged to use renewable energy sources up to a certain percentage for heating and/or cooling of new builds. There are attractive ways to meet these obligations, for example by using a CHP.

Data protection – beware and protect your data

From a data protection perspective, running a data centre is essentially about storing, maintaining and processing digital information. In practice, however, there are many more things to consider, such as knowing your customer (KYC), understanding their needs, providing tailored physical and digital infrastructure as well as suitable software architecture, server capacity and staff. We understand the need to combine both the legal and practical approaches.

After all, adequate data protection and security require a certain infrastructure and highly trained staff. Managing a data centre therefore inevitably involves and rests on a prudent and forward looking privacy concept. To the point internal guidelines as well as comprehensive contractual agreements with suppliers, sub contractors and customers are key in this context. This is what we focus on in our day today advice.

The correct and legally compliant treatment of personal data is only one aspect to be addressed, but is probably the most obvious one. Confidentiality requirements are not merely confined to personal data. There is plenty of digital information stored in data centres that may not be classified as data relating to an identified or identifiable individual, but may still be of crucial economic value to the customer. Prime examples of this are trade secrets and confidential technical information.

Moreover, machine generated data has become increasingly important. The so called "*Internet of Things*" ("**IoT**") is an almost unlimited source of digital information which requires storage and maintenance. Handling such big data and offering services such as text and data mining algorithms is both a technical challenge and a business opportunity. The increasing volume of machine generated data raises a whole new set of questions. Who owns the data (e.g. data collected from cars on the road or home power systems)? What security level should be applied? Is there a public interest in allowing authorities to demand disclosure (possibly through the data centre)? The answers to these questions are still being debated. We advise our clients on exactly these issues.

However, in January the European Commission published the first regulatory initiatives in this area. The legal environment and statutory framework are taking shape and Hogan Lovells is closely monitoring this development. Follow us at www.dsmwatch.com).

The new law

We are currently faced with an environment of change in Europe. The General Data Protection Regulation (GDPR) has been enacted and will take effect as of 25 May 2018. It will replace 28 domestic privacy laws throughout the European Union. National laws will only continue to apply in areas not fully

harmonized by the GDPR. The supervision of privacy compliance will differ from what we have been used to in the past.

Notably, the territorial scope of the GDPR not only covers the activities of an establishment located in the EU. It also applies as soon as the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of behaviour to the extent that it takes place within the EU. This means that processing personal data in data centres may not only allude to EU data privacy law, but also raise a wide array of complex challenges and questions in this field.

In particular in view of the significant sanctions regime – with fines of up to 2 percent of worldwide annual turnover – compliance with data privacy requirements has become even more important to any entity handling person-al data.

However, it should be noted that the GDPR is not the only new piece of legislation governing the storage and processing of data. In January 2017, the European Commission published a proposal for an ePrivacy Regulation. Its core focus is to ensure an adequately high level of confidentiality of electronic communications throughout Europe. In pursuing this aim, the draft Regulation goes beyond purely personal data and covers all kinds of private information. For more details, see our international blog at http://www.hlmediacomms.com.

Data privacy

Having mentioned the new GDPR, it is worth highlighting a few regulatory requirements that are most likely to demand the adaptation of existing technical processes and legal terms and conditions.

The obligations that deserve particular mention include compulsory cooperation requirements with the competent supervisory authorities, notification obligations as regards infringements, data privacy by design and by default, the right to be forgotten and various new documentation requirements. Also, the concept of a data protection officer has been expanded to the entire Union.

It should also be noted that under the GDPR both the controller and the processor are responsible for privacy compliance. Fines for non compliance are substantial, not to mention the damage that would be caused to a company's image if it were accused of failing to meet data protection requirements.

Accordingly, it is crucial to have adequate and upto date privacy concepts in place governing staff, services and infrastructure. Data processing agreements need to be revised and adapted to reflect the new regulations of the GDPR and the coming ePrivacy Regulation. In this context, multiple layers of subcontractors in cloud infrastructures are a particularly common source of difficulty and ambiguity. Clear contractual structures and transparent

technical architectures are recommended safe-guards in this respect.

Different business scenarios

Privacy law generally differentiates between "*controllers*" and "*processors*". A different set of obligations applies depending on which of these two roles a company has. A data centre operator has various options to choose from. The business model chosen by a firm will determine which legal regulations it must meet. Conversely, the respective legal obligations can make certain business models more or less attractive. Therefore, taking an informed decision as to how the data centre service will be structured is essential for business success.

Generally, a distinction can be made between two common business scenarios:

First, **controllers deploying a hosting provider**. Here, processing and infrastructure are part of the service rendered. Whereas the original controller is still regarded as a controller, the hosting provider might either be a processor or a (secondary) controller, depending on the extent of autonomy involved in the service rendered. The service contracts need to be drafted accordingly to ensure adequate justification for the agreed handling of data.

Secondly, **controllers deploying a mere housing provider** providing only the data centre infrastructure. Under a "pure" version of this scenario, i.e. where no (emergency) services that potentially allow access to the processed data are offered by the housing provider, the latter may be deemed neither a processor nor a controller of the data. However, such scenarios rarely exist in practice.

As we have seen, there are various ways to "design" a data centre service and each design brings with it a slightly different set of legal requirements.

Cyber security

Data centres are data hubs and therefore susceptible to cyber attacks. Such attacks could result not only in data theft, but also in the disruption of internet services of multiple customers and businesses. Consequently, a data centre operator faces high liability risks.

There have been many instances of high profile cyber attacks such as:

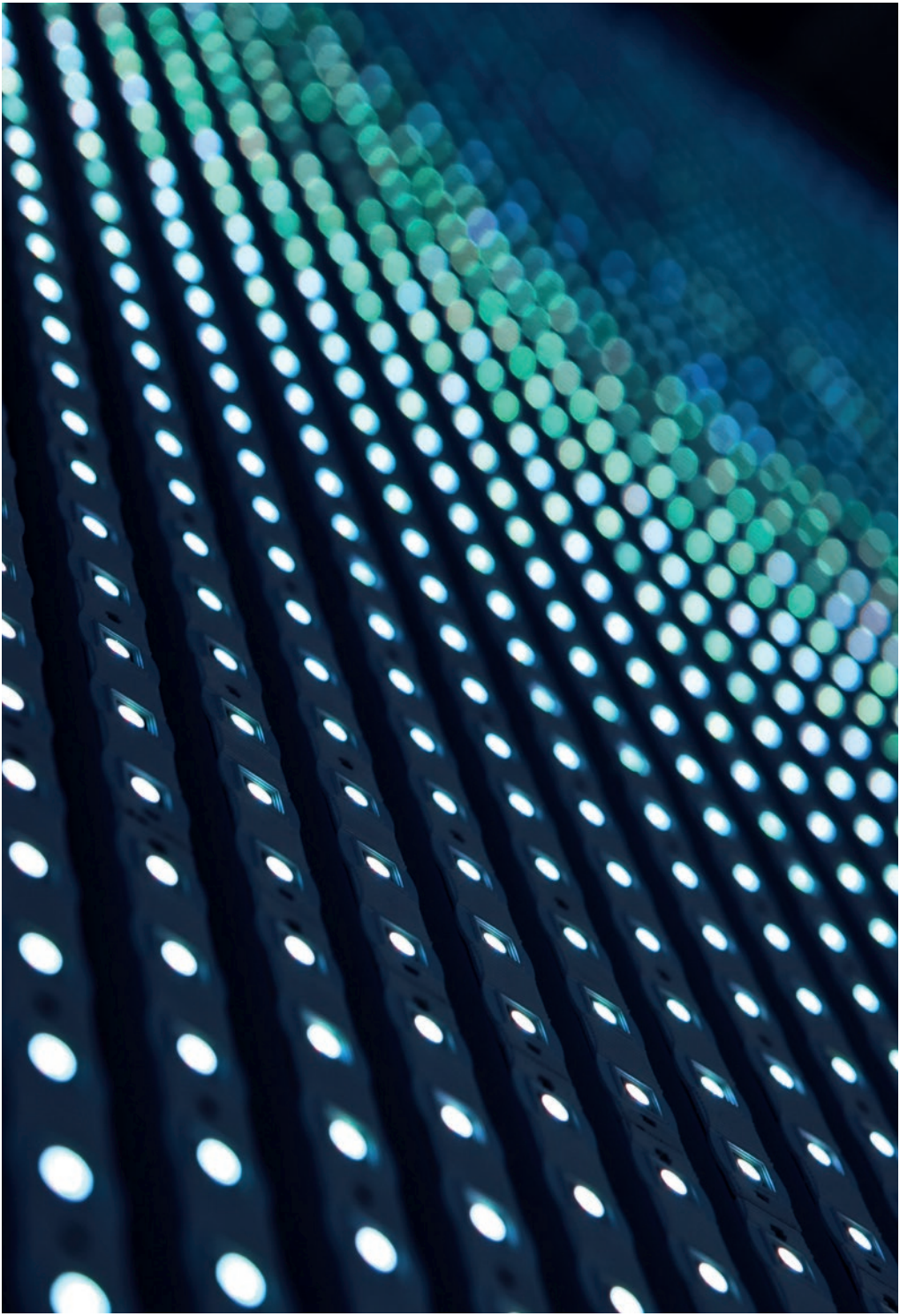
- (Distributed) Denial of Service (DDoS) attacks where servers shut down due to being overloaded by a flood of incoming messages.
- Ransomware attacks, such as WannaCry and NotPetya, where malicious software blocks access to a computer's data, asking for a ransom to release the data or otherwise threatening to destroy it.
- Attacks against the data centre infrastructure to screen, control or eventually destroy the facility such as the Stuxnet virus.

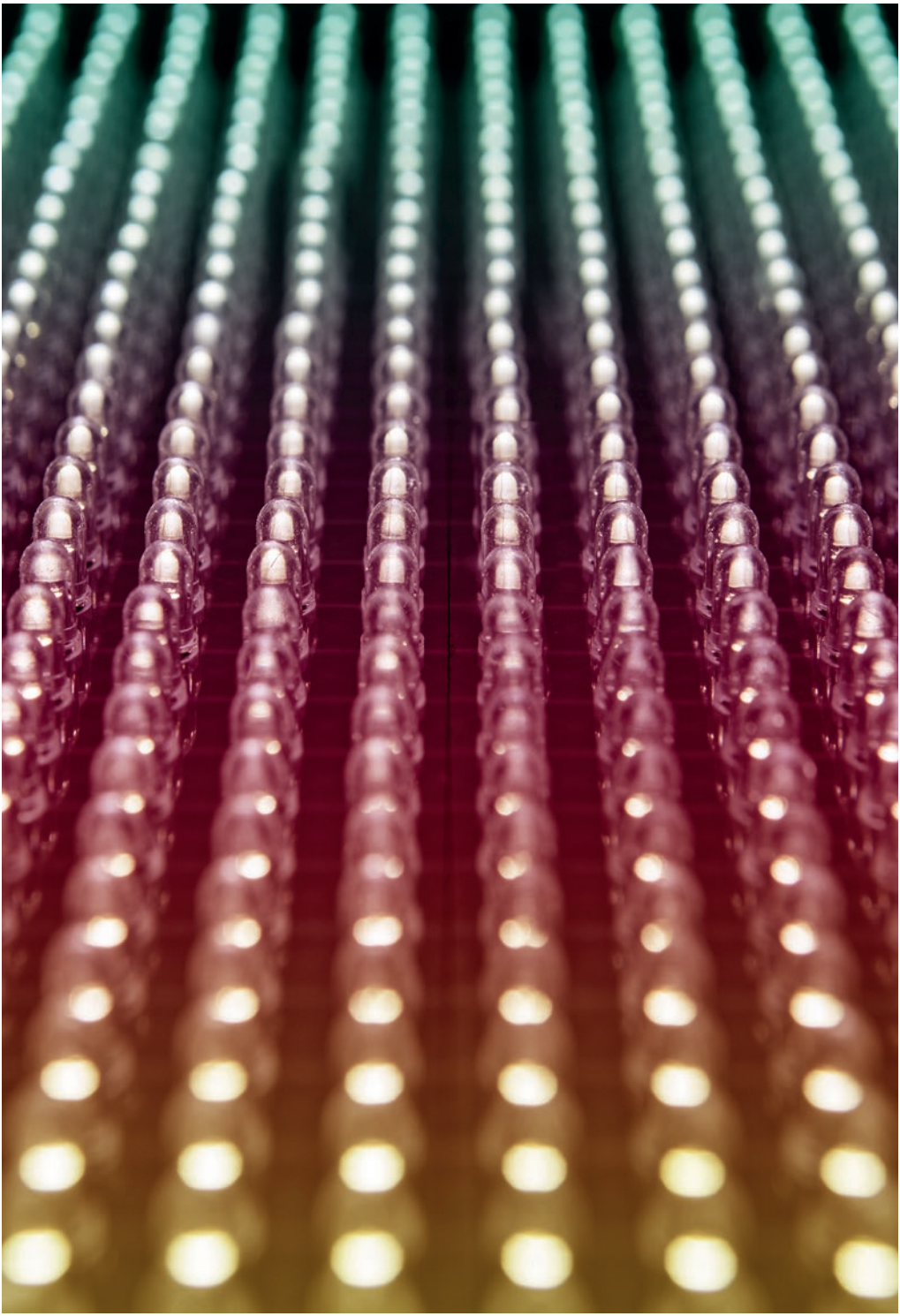
Recently, there has been a noticeable trend toward more sophisticated attacks. Such unprecedented techniques render the data centre infrastructure even more vulnerable and are likely to result in liability claims by the data centre's customers.

Unpredictable and unforeseen incidents – also known as black swan events – may not necessarily trigger fault based liability of the data centre operator. However, it can be very challenging and practically impossible for the operator to prove the existence of such a black swan event. The WannaCry and NotPetya incidents illustrate that threat actors exploit malware families and reuse efficient attack strategies. Considering the nature of cyber attacks, it is notable that, e.g. in Q1 and Q2 2017, 75% of all ransomware attacks were based on the same six known malware variants. This means that, had the proper security mechanisms been in place, these threats could have been prevented. In such cases, data centre operators may not be able to be released from nonfault liability; as such events could have been prevented and are not to be considered as black swan events. The data centre operators may thus be held liable. Therefore, it is strongly recommended that data centre operators stay informed about current threats and cyber security trends. Otherwise, the data centre's board faces personal liability or regulatory fines.

Hence, more efficient security packages or change of outdated IT infrastructure may be advantageous to such operators. They might result in higher costs, but augmented liability and negative publicity can lead to more severe problems.

Certain data centre operators might also be subject to stricter regulation. Data centres with an annual performance of more than 5 Mega watt, IT hosting with more than 25,000 annual average instances, content delivery networks with an annual data volume of 75,000 TByte, trust services with more than 500,000 issued qualified certificates or 10,000 certificates for authentication of publicly available servers are subject to the German Federal Agency for Security in Information Technology Act (BSIG). As a result, sector-specific security standards (*Branchenspezifische Sicherheitsstandards* – B3S) apply. The B3S for data centres, however, are based on ISO family 270xx. Especially the ISO 27001 and ISO 22301 – in addition to the other data centre specific security standards – are referenced and need to be respected and implemented by the data centre operator.





Data centre projects and transactions – our expertise

Our credentials

At Hogan Lovells we have a great depth of experience in advising clients on the establishment and acquisition of data centres.

The value we bring to clients is both in the depth of expertise in critical subject areas, such as telecommunications regulation, real estate and land use law and regulation, tax, employment, and environmental regulation, and in our ability to co-ordinate this advice across jurisdictions, exercising sound judgment in supporting clients with location selection decisions and strategies for execution. We have strong relationships with local regulators and we understand the markets in which our clients operate.

More than just data storage

We have experienced projects, real estate, corporate, and commercial teams who can assist

- with all aspects of the acquisition and construction of data centre sites or
- fully operating data centre businesses if required
- with establishing title and ownership
- with all aspects of data centre transactions and ongoing operation, including site suitability and risk factors, planning and environmental issues, ownership of key infrastructure (e.g. backup power, cooling, and fire suppression, customer contracts)

Setting up a data centre also has various tax implications for the provider as well as for potential customers which should be taken into account (e.g. permanent establishment aspects, VAT aspects). Our Tax team is highly experienced in setting up tax efficient structures and dealing with all relevant tax aspects in the respective agreements.

Our services

- Industry specific due diligence
- Real estate and regulation
- Service – and O&M-contracts
- Energy-related advice and cost efficiency
- Coordination of global deals as your single-point-of-contact in Germany
- Finance
- Commercial and tax

Our distinctive expertise

Keppel Telecommunications & Transport and Alpha Investment Partners

On the acquisition of a EUR 76m data centre from Citigroup and on the sale-and-lease back agreement to Citigroup who remains the tenant.

Keppel DC REIT

On its acquisition of a data centre in the Celtic Gateway Business Park. The data centre is fully let to one of largest global cloud service providers on a 15-year full repairing and insuring lease that commenced in June 2016.

A borrower

The borrower in a (re)financing of a data centre in Frankfurt.

Telehouse Holdings Ltd. and KDDI

Corporation on its acquisition of Databurg GmbH.

TelecityGroup

- In relation to its acquisition of the Manchester based carrier neutral data centre.
- On its GBP 87.6m acquisition of Data Electronics Group.
- On its acquisition of leading Finland data centre operator Tenue Oy.
- On the acquisition of Academica, a leading data centre and IT services operator in Finland.
- On the acquisition of the data centre business of MedioSystems, an affiliate of the IBM Group.
- On its acquisition of the entire issued share capital of SadeceHosting.
- On its acquisition of the entire issued share capital of 3DC by TelecityGroup International Limited. Hogan Lovells advised On English law and oversaw local advisors.
- On its acquisition of Plix.

A leading UK based operator of data centres

On various project developments (EPC, O&M) as well acquisition of such data centre in Germany.

A UK clearing bank

On the development of a dedicated data centre and a number of consequent upgrade projects.

A major European colocation space provider

On the development of a new data centre and consequent extension project and on projects to upgrade equipment on existing operational sites.

Du Pont Fabros Technology

On its proposed purchase and redevelopment as a data centre of a heavily contaminated former chemical and pharmaceutical manufacturing site.

A leading global bank

On establishing a data processing subsidiary in China.

A leading data centre operator

On the acquisition of the reversion to their facility in Harbour Exchange Canary Wharf, regearing followed by sale and leaseback.

A leading data centre operator

On the lease review of 46 leases across 6 countries for a leading data centre operator.

One of Europe's leading data centres

On all employment matters across Europe.

A number of financial institutions

On fit out of new UK headquarters premises, with related internal data centres.

Your key contacts

Dr. Tobias Faber
Partner, Frankfurt

Dr. Alexander Stefan Rieger
Counsel, Frankfurt

Dr. Fabian Pfuhl
Counsel, Frankfurt

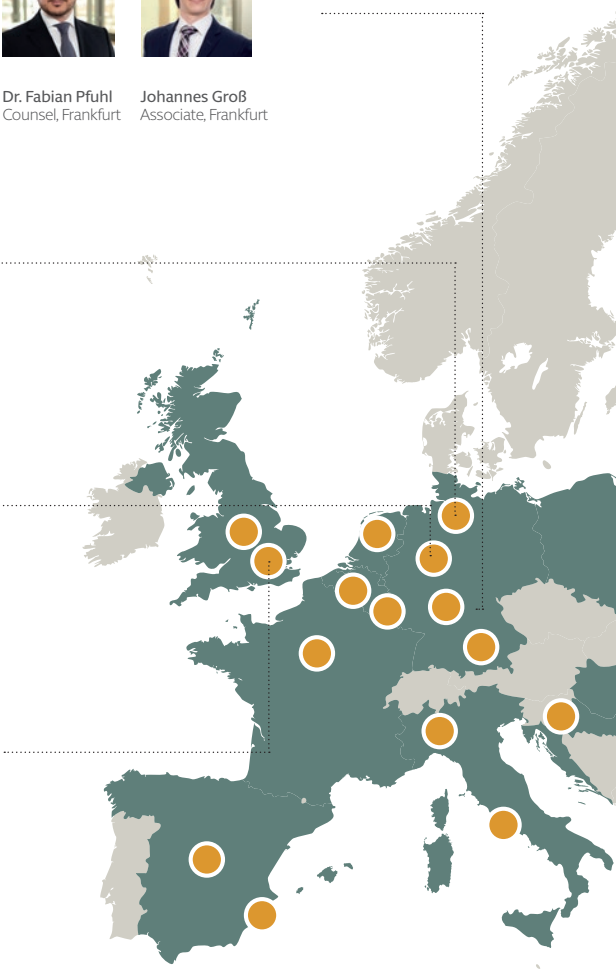
Johannes Groß
Associate, Frankfurt

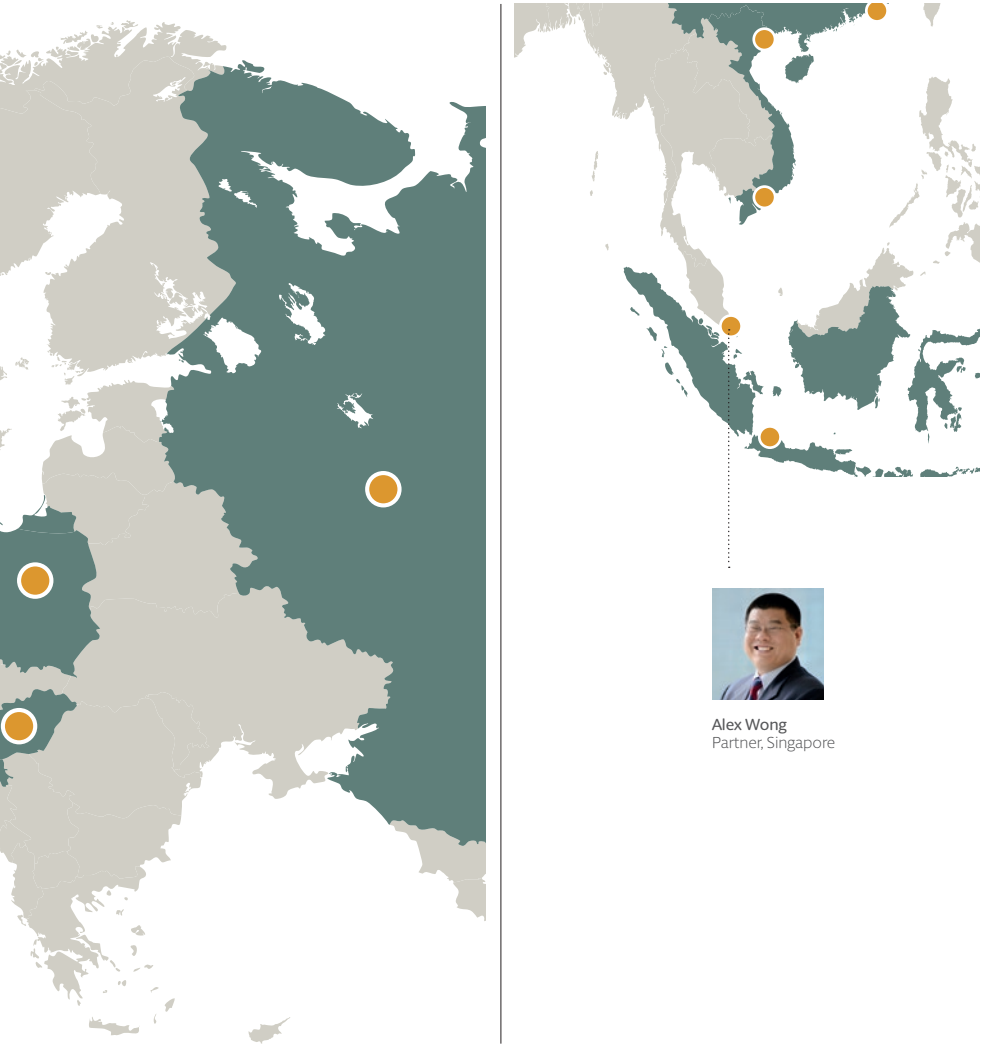
Dr. Carla Luh
Partner, Hamburg

Dr. Mathias Schönhaus
Counsel, Dusseldorf

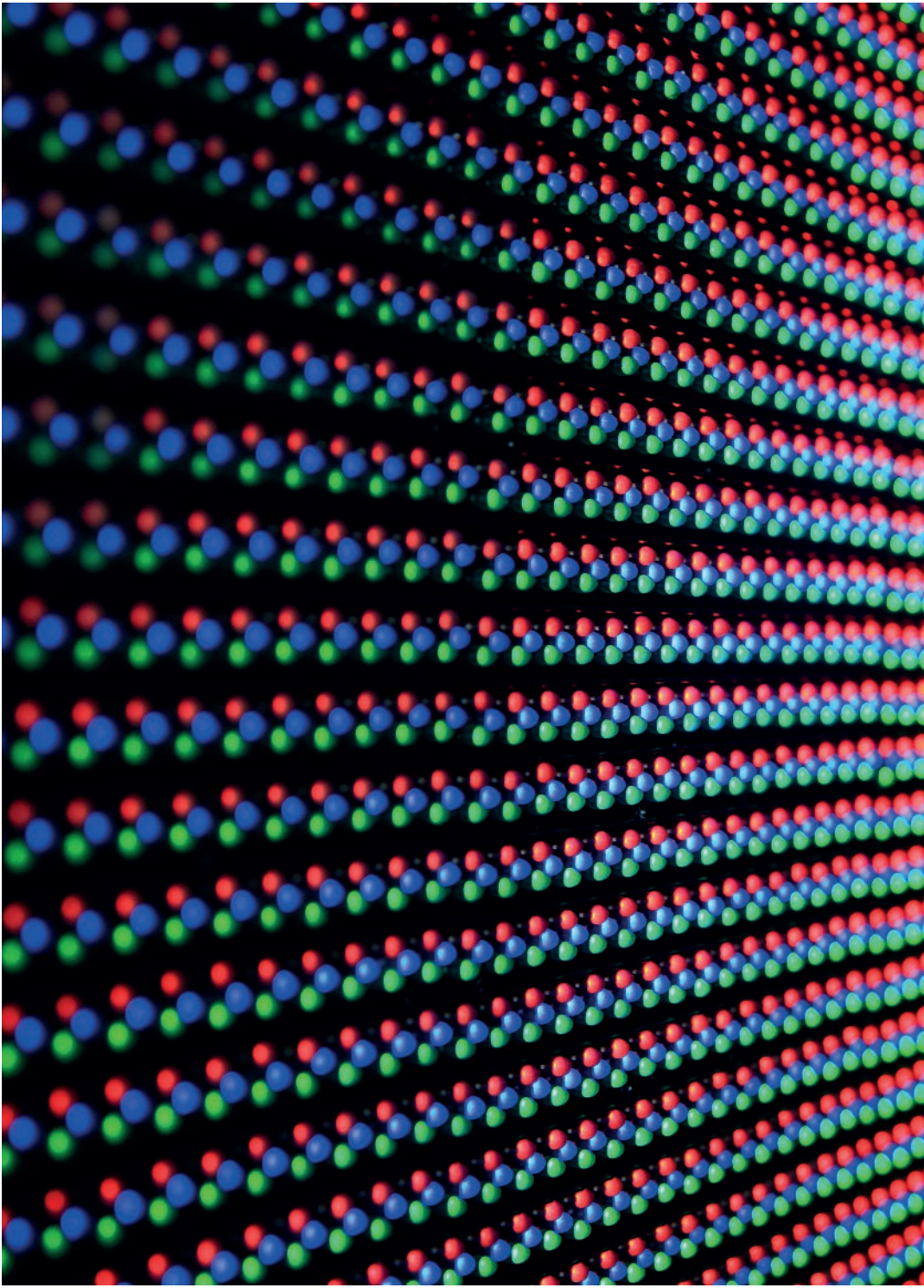
Dion Panambalana
Partner, London

Nicola Evans
Partner, London





Alex Wong
Partner, Singapore



Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

www.hoganlovells.com