Cloud Computing 2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2017
Fifth edition
ISBN 978-1-83862-634-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Cloud Computing
2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston
Bryan Cave Leighton Paisner LLP

Lexology Getting The Deal Through is delighted to publish the fifth edition of *Cloud Computing*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston of Bryan Cave Leighton Paisner LLP, for their assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
September 2021

Contents

United Kingdom

Marcus Pearl and Anna Blest*

Bryan Cave Leighton Paisner LLP

MARKET OVERVIEW

Kinds of transaction

1 What kinds of cloud computing transactions take place in your jurisdiction?

As a G7 economy with mature information technology and related services markets, the United Kingdom is a significant global market for cloud computing. According to Gartner, judged by cloud spending rates and growth, the United Kingdom is among the fastest cloud adopters globally, ranking behind the United States (the world leader in cloud adoption since 2015) and Canada. In its 2018 Global Cloud Computing Scorecard (the most current version since its first publication in 2012, and which claims to be the only global report to rank countries' preparedness for the adoption and growth of cloud computing services), BSA|The Software Alliance ranks the UK fourth after Germany, Japan and the United States. To account for the difference in the UK's standing in these two reports, it is worth explaining that the BSA's scorecard is based on a methodology that emphasises policy areas that 'matter most to cloud computing', such as data protection and privacy laws, cybersecurity regimes and intellectual property protection (ie, the effectiveness of the legal and regulatory environment for cloud computing). And it also applies a test of IT infrastructure readiness, in particular access to broadband. However, a 2019 CloudPro survey discussed in TechUK's 'Cloud 2020 and beyond: Unlocking the power of the cloud' report ranked the UK sixth in the European Union for the adoption of cloud services, behind the Scandinavian countries but ahead of France and Germany.

Other market analysts, such as MarketsandMarkets, observe that successful implementation of the UK's National Broadband Plan has resulted in faster mobile data connection speeds in the UK, which in turn has facilitated a faster adoption of cloud services in the United Kingdom. The government's stated ambition is to increase the availability of full-fibre and 5G networks. The National Infrastructure Strategy was published in November 2020, announcing a £5 billion investment to support UK-wide gigabit broadband roll-out (Project Gigabit), an initiative to extend 4G mobile coverage to 95 per cent of the UK, and a £250 million investment to ensure resilient and secure 5G networks. The transition to cloud services is supported and encouraged by the UK government. The government has collaborated with leading cloud providers such as IBM and Microsoft to promote and accelerate cloud adoption in the public sector. In addition, it has published guidance and declarations to aid cloud adoption as well as launching initiatives such as the Digital Marketplace to assist public sector organisations in procuring cloud technologies.

Using the US National Institute of Standards and Technology (NIST) definition of cloud computing, there is extensive use of the three NIST service models: software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS), referred to below as 'service models'. Of the four NIST deployment models (private cloud, community cloud, public cloud and hybrid cloud), private, public and hybrid clouds are widely adopted. Community clouds are also used, although less regularly.

As part of the UK's cloud business ecosystem, there are cloud service brokers (providers who aggregate several different cloud services to provide a unified offering to a customer) and cloud exchanges (providers that offer direct connections between several cloud platforms, providing their customers with access to and portability among separate cloud platforms, without their data passing through the internet). 'Cloudbursting' – in the context of the hybrid deployment model, with customers moving specific processes running in-house to public cloud services to provide greater capacity – has become more common.

A notable feature of the UK market is the adoption by central and local governments of the G-Cloud framework, which enables government departments and state agencies to buy and deploy cloud services from pre-approved vendors, which include some of the biggest cloud providers, such as Amazon Web Services (AWS). The UK government's Cloud First Policy was reassessed in 2019 and remains a flagship technology policy. This requires public sector organisations to consider and evaluate potential public clouds as a deployment model, before considering any other IT option. Cloud First has been mandatory for central government departments and agencies but has been strongly recommended to the wider UK public sector. The latest iteration of government guidance is contained in 'The One Government Cloud Strategy', which was last updated in February 2021. The National Cyber Security Centre's current Cloud Security Guidance (published 2018) reflects support for the Cloud First Policy. Public and third sector organisations that want to purchase high volume cloud hosting solutions flexibly can now do so through a new £750m Crown Commercial Service framework called Cloud Compute. Nine cloud service providers have been chosen to support customer requirements via Cloud Compute. This framework (unlike G-Cloud) allows customers to rapidly scale up or down their usage as and when required, with longer call-off options than other cloud agreements. It covers IaaS and PaaS requirements and focuses on flexible computing environments, such as those used for the development of new software applications or where large and complex data sets need to be modelled. The framework will run for four years. Call-off terms are up to three years, with two possible extensions of up to 12 months each.

Recent research has shown that 78 per cent of UK public sector organisations are using some form of cloud-based service, compared with only 38 per cent in 2010. However, although the adoption of cloud services by UK local governments still lags behind the central government's rate of deployment, the adoption rate at the local government level is apparently steadily increasing. A 2021 survey showed that whilst the large majority of councils store their data on-premise, 74 per cent also use some form of cloud to store data, with over 69 per cent using public cloud and just over half using private cloud. UKCloud's 2020

survey reported very high levels of public sector interest in shifting to cloud solutions, but that respondents still remained concerned about the commercial risks of single provider solutions, with over-reliance on a single provider inhibiting cloud adoption; operational and security risks in using a public cloud; and the cost or affordability of cloud solutions. There is a growing trend in customer use of hybrid or multi-cloud strategies, driven by cost and performance objectives, to avoid the risk of vendor lock-in. This allows a customer greater flexibility in moving workloads between cloud providers and potentially reduced costs by not relying on a single provider for fees and terms and can improve latency by avoiding being tied to the availability and location of the data centres of a single public cloud provider. If multiple cloud providers are used, the number of available virtual machines and proximity to locations can improve.

The Flexera State of the Cloud Report for 2021 reported that public cloud adoption continues to accelerate, with 90 per cent of respondents expecting cloud use to exceed plans due to the pandemic. There has been increasing uptake of multi-cloud strategy with 92 per cent of respondents using a multi-cloud strategy, using on average 2.6 public and 2.7 private clouds. Flexera's survey showed that 99 per cent of respondents are using at least one public or private cloud and respondents are running 50 per cent of their workloads in public clouds, with this likely to increase in the coming year.

With the UK being one of the most advanced global markets for cloud computing, there is a sizeable business ecosystem serving the primary market, for example, in data centres, which is predicted to be a significant growth area in the period 2021-2026 in the UK. Notable transactions in the UK in 2021 included NHS Scotland's partnership with AWS, the Premier League partnering with Oracle, AWS joining the One Government Value Agreement under a three-year memorandum of understanding and the UK central government transferring crucial services to Oracle. SAP also announced the launch of a secure UK-based cloud service as part of a five-year investment package worth €250 million (approximately £212 million). The SAP UK Data Cloud is a cloud infrastructure for the public sector and will combine SAP's partnerships with AWS, Azure and Google Cloud with UK data centres to launch an in-country cloud. This will support critical UK national infrastructure in healthcare, transport, education, policing and utilities, as well as central and local government operations.

Active global providers

2 | Who are the global international cloud providers active in your jurisdiction?

A small sample of the providers active in the UK, include the following:

- Accenture;
- Adobe;
- Alibaba Cloud;
- AWS;
- Avaya;
- Basecamp;
- Cisco;
- Citrix;
- Dell EMC;
- Dropbox;
- Equinox;
- Facebook;
- Google;
- GTT Communications;
- Huawei;
- IBM;
- IDC;
- iCloud;
- Joyent;
- Kaspersky;
- Microsoft;
- NetApp;
- Oracle;
- Rackspace;
- Red Hat;
- SalesForce;
- SAP;
- SAS;
- Skype;
- Sungard;
- Symantec;
- Tencent Cloud;
- VMware;
- Webex; and
- Workday.

See also CloudPro's list of providers.

AWS, Google Cloud and Microsoft Azure are the leading IaaS providers in the UK.

Active local providers

3 | Name the local cloud providers established and active in your jurisdiction. What cloud services do they provide?

The following is a small, illustrative, selection by service segment:

- server, storage and infrastructure: ElasticHosts, Fasthosts, Flexiant, BT Cloud, UKFast eCloud, Memset, Zsah Limited and Stone Group;
- managed services: BT, Claranet, Colt, Interoute, iomart, IT Lab, Nasstar, TIG and CWL Systems;
- data backup and security: BT, Cloud Direct, iomart, IT Lab, Memset, TIG, UKFast, UK2 and Vodafone;
- hosted desktops: Colt, Nasstar and Vodafone; and
- channel enablement, go to market, digitisation, and customer relationship management: BCSG and NewVoiceMedia.

See *Computer Weekly's* 'UK hosted desktop cloud providers' (however, this study was undertaken in 2010 and has not been updated), and Cloud Tango's list of its UK Top 50 managed service providers. For various cloud services mainly focused on the UK public sector, there is UKCloud.

Market size

4 | How well established is cloud computing? What is the size of the cloud computing market in your jurisdiction?

A report from Research and Markets' Cloud Computing Market by Service Model, Deployment Model, Organization Size, Workload, Vertical and Region – Global Forecast to 2023 estimated that the global value of cloud services could grow by an annual rate of 18 per cent between 2019 and 2023.

Anecdotally, the impact of covid-19 has been to accelerate the uptake of cloud services, with research estimating that it has advanced cloud adoption by three to five years. According to a market survey undertaken by EY, UK banks are starting to embrace the move to cloud computing, as 27 per cent plan to migrate 50 per cent or more of the business in the next two years. The ambition towards moving to cloud services has been prompted by the covid-19 crisis, which pushed banks to prioritise cloud adoption strategies. However, there is still a long way to go for UK banks to fully embrace cloud adoption.

The 2021 'State of Digital and Data' report published by UKcloud, which surveyed over 300 public sector organisations, reported that 58

per cent of respondents said their data is in the public cloud, with 56 per cent noting that their data is spread across multiple cloud services. The report highlighted the awareness organisations have gained in 2020-2021 as regards the benefits of adopting cloud services, with 60 per cent of the respondents expressing a desire to transfer all their data to cloud services.

Interestingly, AWS polling research suggests there is a significant regional disparity in cloud uptake across the UK. For example, 52 per cent of companies in Greater London reported using cloud platforms, whereas only 25 per cent of companies reported the same in the East Midlands.

Impact studies

5 Are data and studies on the impact of cloud computing in your jurisdiction publicly available?

Authoritative, specific and recent data on the true size and therefore impact of cloud computing in the UK is hard to find. And such reports do not tend to be freely available to the general public, online or otherwise. The report from Research and Markets' Cloud Computing Market by Service Model, Deployment Model, Organization Size, Workload, Vertical and Region – Global Forecast to 2023 is the most specific and authoritative by reference to the size of the UK cloud market generally, and by reference more specifically to the cloud service and deployment models. We anticipate that new data sets will be available later in 2021, which will also reflect the impact that the increased use of remote working due to the covid-19 pandemic has had on organisations' adoption and use of cloud technologies. Current data available is focused on the global cloud computing market and does not tend to split out revenues received by the larger providers by geography. AWS has produced a recent report on the impact it has had in the UK.

POLICY

Encouragement of cloud computing

6 Does government policy encourage the development of your jurisdiction as a cloud computing centre for the domestic market or to provide cloud services to foreign customers?

In short, yes. The policy manifests itself in various forms and initiatives, but comprehensive coverage of them is beyond the scope of this chapter.

The starting point is the government's policy paper, UK Digital Strategy 2017, published on 1 March 2017 by the responsible government department, the Department for Digital, Culture, Media & Sport. In April 2017, the Digital Economy Act 2017 was enacted to implement the government's digital strategy. It is clear from the UK's digital strategy, the Digital Economy Act 2017 and examples of government support given directly or indirectly to cloud computing and cloud-enabled organisations, that the policy and implementation framework embraces all the cloud service models and deployment models. This was followed by the UK's National Data Strategy, published in December 2020, and the subsequent response to a consultation. This focuses on five core missions:

- unlocking the value of data held across the economy to drive innovation and research;
- securing a pro-growth and trusted data regime;
- transforming government use of data to drive efficiency and improve public services (which includes delivery of a new Integrated Data Programme, trialling secure cloud-native architecture);
- ensuring security and resilience of infrastructure (such as data centres, recognised as critical to protecting the security of the digital supply chain); and
- championing the international flow of data.

The UK government is a world leader in its deployment of cloud computing through its Government Cloud First Policy. In October 2019, the government reaffirmed the Government Cloud First Policy would remain a flagship technology policy, after some speculation that it would be replaced. The G-Cloud 12 framework, which supports UK public sector bodies to buy cloud computing services, was launched in September 2020 and will end in September 2022 (pre-market engagement on its replacement, G-Cloud 13, is taking place at the time of writing). It is also supporting the Cloud Compute initiative, which launched in Spring 2021.

The National Cyber Security Centre has issued guidance for customers procuring cloud services that looks at how to configure, deploy and use cloud services securely. In May 2021, the government also issued a call for views on cybersecurity in supply chains and managed service providers, emphasising that 'digital is at the top of the government's agenda [and it] has made digitally-driven growth a priority, and has set out ambitions to drive use and implementation of the latest technology in infrastructure, boosting cyber skills, and creating innovative technology sectors and businesses across the country', while acknowledging that supplier risk management and assurance is challenging for businesses.

There is potential for the new 2021 National Investment & Security Act to impact investments made in the UK cloud sector, where an investment gives rise to national security concerns. Any share acquisitions with a UK nexus entered into from 4 January 2022 in 17 key sectors (including computing hardware, artificial intelligence, communications, data infrastructure and critical suppliers to government), and which give rise to an increase in holdings or voting rights beyond thresholds of 25 per cent, 50 per cent, 75 per cent or sole ownership, will be subject to prior review and approval by the new Investment Security Unit within the Department for Business, Energy & Industrial Strategy. The mandatory filing regime is set to have broad application and will be triggered by deals of any value, and where a target entity's connection with the UK may be limited (eg, only having supply relationships with UK customers). Completing a qualifying transaction in a key sector without pre-approval will amount to criminal and civil offences and the transaction will be void. Government guidance indicates that the regime is likely to have broad extraterritorial scope.

Incentives

7 Are there fiscal or customs incentives, development grants or other government incentives to promote cloud computing operations in your jurisdiction?

Yes. In its 2020 Budget, the government announced public investment in R&D would increase to £22 billion per year by 2024 – 2025, although this will cover general R&D, of which cloud computing is a part. Although in most cases, cloud computing is not specifically mentioned and eligibility for fiscal benefits, funding and other incentives will depend on specific criteria for particular applications and uses of ICT, it is clear that the incentives do extend to cloud computing and individual elements of it. Broadly, these incentives are directed at start-ups and early-stage companies. They generally cover tax incentives for the companies and their investors, grant funding, contributions towards running costs, and start-up and later-stage corporate development loans.

Specifically, these incentives include the following as a representative sample.

The Seed Enterprise Investment Scheme

The Seed Enterprise Investment Scheme offers tax-efficient benefits to investors in return for investing in small and early-stage start-up technology businesses in the UK.

The Enterprise Investment Scheme

The Enterprise Investment Scheme offers tax benefits to investors in technology companies.

Research and development tax credits

R&D tax credits are available for both small and medium-sized enterprises (SMEs) and larger companies (at different levels), comprising a tax credits regime for qualifying R&D relating to assets developed for internal use, which may include subcontractor costs, supporting software and software-as-a-service (SaaS), and some hardware costs. However, general hosting and cloud computing costs do not fall into any of these qualifying areas specifically, and companies have to apportion expenditure between qualifying and non-qualifying costs.

The government increased the Research and Development Expenditure Credit in its 2020 Budget, from 12 to 13 per cent. The 2021 Budget specifically stated that it will consider bringing data and cloud computing costs into the scope of R&D tax relief schemes, with the objective of ensuring the United Kingdom remains a competitive location for cutting edge research. Its March 2021 consultation indicated that it recognises the case for widening the scope of expenditure which attracts relief, when there is a qualifying R&D activity, to include data and cloud computing. It also announced the launch of Future Fund: Breakthrough, which is a £375 million funding programme to encourage private investors to co-invest in high-growth, innovative R&D-intensive businesses.

The Patent Box

The Patent Box scheme enables SMEs and larger companies to apply a lower rate of UK Corporation Tax to profits earned after 1 April 2013 from their patented inventions.

Innovation funding

For innovative products, processes or services, funding of between £25,000 and £10 million is available.

Innovate UK runs funding competitions for projects led by UK-based companies. As of July 2021, competitions include the opportunity to apply funds to develop automated vehicles and for a share of up to £25 million to deliver 'ambitious' or disruptive R&D innovations that can make a significant impact on the UK economy.

The British Business Bank and enterprise capital funds

The British Business Bank invests alongside venture capital funds (partners) under a rolling programme. Funding is aimed at smaller UK growth companies.

On 31 March 2020, the government published all its guidance on cloud computing in the public sector in one place, to improve support and make adoption of cloud computing easier.

LEGISLATION AND REGULATION

Recognition of concept

8 | Is cloud computing specifically recognised and provided for in your legal system? If so, how?

Not specifically, other than in the Network and Information Systems Regulations 2018, although it is clear that English consumer, commercial, regulatory and competition law is intended to apply to cloud service providers.

Governing legislation

9 | Does legislation or regulation directly and specifically prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Yes, in respect of cybersecurity and resilience and cyber incident reporting. The Network and Information Systems (NIS) Regulations 2018, which implement the EU NIS Directive (2016/1148/EU), specifically govern 'cloud computing services' meaning 'digital services that enables access to a scalable and elastic pool of shareable computing resources' (Regulation 1(2)).

Cloud service providers (CSPs) that fall within the definition of a 'relevant digital service provider' (RDSP) must, broadly stated, take appropriate and proportionate technical and organisational measures to prevent and minimise the impact of cyber incidents and related risks to their system. The regulations deal with any incident that has an impact on a service, where that impact produces a significant disruptive effect (and while this includes cybersecurity incidents, it also extends to non-cyber events that have an impact on systems). RDSPs are also required to notify the UK Information Commissioner's Office (ICO), the regulator for these purposes, of any incident that has a substantial impact on the provision of the cloud services within 72 hours. The ICO has a range of enforcement powers, including the right to issue financial penalties for material contraventions, up to a maximum of £17 million. RDSPs were required to register with the ICO by 1 November 2018. There are exceptions for, among others, small or micro-businesses. To be subject to the NIS for UK regulatory purposes, a CSP must have a head office in the UK (or a nominated representative), more than 50 staff and a turnover or balance sheet of more than €10 million.

The ICO has issued a detailed and helpful guide to the NIS Regulations, which all CSPs operating in the UK should consult as a first step. The Guide includes pointers to the cloud services to be governed by the regulations. The guide states that platform-as-a-service and infrastructure-as-a-service models will be covered, but that software-as-a-service will only be regulated to the extent that the service is 'scalable and elastic' and fulfils a business-to-business function. The UK National Cyber Security Centre's guidance should be consulted.

The UK's National Security and Investment Act 2021 may restrict parties acquiring shareholdings in CSPs, where this has a potential impact on the UK's national security (depending on the interpretation of the 17 key sectors for which regulatory oversight by an Investment Security Unit will now be required before a transaction can proceed). As the framework is new and comes into force on 4 January 2022 (however, certain aspects will apply retrospectively), transactions involving the acquisition of cloud businesses should be scrutinised carefully, as failure to comply with the notification requirements required by the National Security and Investment Act could amount to criminal and civil offences and the transaction will be void.

10 | What legislation or regulation may indirectly prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

In the UK, as business-to-consumer (B2C) and business-to-business (B2B) IT services, cloud computing services will, depending on the scope of the services and the circumstances and context of their supply, be subject to the legislation and regulation that apply to all similar IT services. Given the breadth and complexity of the cloud computing business in the UK, other participants in the provision of elements of cloud infrastructure and in the cloud supply chain may be subject to that legislation and regulation, too, for example, a communications service provider supplying a transmission service enabling the CSP to communicate with a cloud customer or the provider of cloud servers to a CSP.

As such (and with applicable B2C cloud computing consumer protection measures and data protection law), the following are likely to apply to cloud computing (or elements of it) in the UK:

- Digital Economy Act 2017;
- Regulation of Investigatory Powers Act 2000 (as amended) and Investigatory Powers Act 2016 (as amended) – interception of communications and retention of communications data, etc;
- EU Dual-Use Regulation 2009, Council Regulation (EC) No. 428/2009 (and associated legal amendments) – regulates the export of dual-use technologies and software;
- Export Control Order 2008 (as amended) – controls on the export of military and certain other technologies and software;
- Communications Act 2003 – overall regulatory structure and powers for communications and media in the UK, including the communications and media regulator Ofcom;
- Export Control Act 2002 – controls on the export of, among others, strategic technologies;
- Unfair Contract Terms Act 1977 – makes certain terms in B2B contracts that do not satisfy the requirements of 'reasonableness' unenforceable; and
- Privacy and Electronic Communications Regulations 2003/2426 (as amended) and the Platform to Business Regulation (2019/1150), implemented in English law via the Online Intermediation Services for Business Users (Enforcement) Regulations 2020 (SI 2020/609) – requires online intermediation service providers (eg, providers of online e-commerce marketplaces, software apps and social media services) and online search engines to comply with certain transparency obligations, mainly by including information in their terms and conditions or, for search engines, publishing it on their websites.

The above is not an exhaustive list, and readers should also consider other areas covered by UK legislation and regulation, including those regarding intellectual property rights, insolvency, consumer protection and employment law.

Apart from legal and regulatory enactments, particularly in the context of cloud computing, readers should be aware of various international law enforcement measures under treaties and applicable EU measures that are likely to be relevant. These generally relate to cybercrime, criminal investigations and enforcement, and inter-state mutual legal assistance in criminal matters. Examples are:

- the Council of European Convention on Cybercrime 2004, ETS No. 185;
- the Agreement on Mutual Legal Assistance between the European Union and the United States, signed 25 June 2003; and
- the United Kingdom's proposed bilateral ratification of the Agreement on Mutual Legal Assistance between the EU and the US, signed 25 June 2003.

Although beyond the scope of this section, readers will be aware of the extraterritorial impact of the USA PATRIOT Act on cloud services.

To give readers a complete view, the same rules and principles (including as to liability) that apply to consumer and commercial technology-related services contracts under the three UK jurisdictions (England and Wales, Scotland and Northern Ireland) will apply to cloud computing contracts, subject to the scope of the services and the circumstances and context of their supply.

Although it is not legislation or public regulation, for the reasons given below, the Cloud Industry Forum's Code of Practice for Cloud Service Providers (CIF Code) is relevant. Its stated purpose is 'to bring greater transparency and trust to doing business in the cloud'. The CIF Code could influence the choice of CSP by potential customers, whether consumers or commercial organisations. CSPs claiming compliance with the CIF Code and the right to use CIF certification may, for validated infringement, face sanctions by CIF, including publication of the CIF's findings on its website and press releases. So while the CIF Code does not have any public legal effect, it may be normative to the conduct of CSPs and it may influence the choice of CSP by commercial end-users and consumers, as well as the public's view of certain CSPs, especially those who have contravened the CIF Code.

Finally, the role of the UK Advertising Standards Authority (ASA) is important in the fast-growing cloud services market. The ASA's role is to ensure that all advertisements are 'legal, decent, honest and truthful'. The ASA publishes codes that it administers and under which it hears and rules on complaints. ASA rulings are published weekly and are 'a transparent record of what is and isn't acceptable' in advertising. The rulings can remain on the ASA's website for five years. Though ASA rulings do not have any legal effect, an adverse ruling may have a significant commercial impact, especially if a business is seen to be disregarding rules designed to protect consumers. And, as a last resort, if advertisers persistently break the ASA codes and are unwilling to change their practices, the ASA states that it can and does refer those advertisers to enforcement agencies that do have legally enforceable powers and the ability to impose legal sanctions for further action (eg, UK Trading Standards or the communications regulator Ofcom). It is worth noting that the ASA has considered several specific cloud computing-related advertisements and found against the advertisers.

In July 2021, the UK government issued a digital regulation policy paper that may lead to regulatory changes for CSPs. Also, in April, it established the Digital Markets Unit, which will oversee a new regulatory regime for digital firms. The Digital Markets Unit has been established within the Competition and Markets Authority on a non-statutory basis, conducting preparatory work ahead of the necessary legislation being passed to grant it powers. The UK government is consulting on those powers and will legislate when parliamentary time allows. The unit is supported in its work by the Digital Regulation Cooperation Forum, which is comprised of the CMA, Ofcom, the ICO and the Financial Conduct Authority.

The impact of the UK's National Security and Investment Act 2021 may also restrict the UK cloud computing market, if, in practice, it limits investment in cloud businesses.

Breach of laws

11 What are the consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing?

For laws and regulations, the consequences of breach range from contractual unenforceability and civil enforcement remedies to criminal and regulatory fines, penalties and other sanctions. In some situations, company directors and senior executives may face personal sanctions.

Consumer protection measures

12 What consumer protection measures apply to cloud computing in your jurisdiction?

For B2C cloud computing arrangements, the following main consumer protection measures will apply.

- the Electronic Commerce (EC Directive) Regulations 2002;
- the Consumer Protection from Unfair Trading Regulations 2008;
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013; and
- the Consumer Rights Act 2015.

These now constitute 'Retained EU law' and will therefore form part of English law unless and until the UK government legislates further in

this area. Together these cover matters including distance selling, the provision of certain information to consumers, marketing and marketing claims, onerous and unfair contract terms and how they are presented, cancellation rights, cooling-off periods, choice of law and venue for consumer litigation (eg, standard terms seeking to impose compulsory arbitration against consumers may be regarded as unfair terms CRA 2015, Sch.2, 20(a)).

Other legislation includes:

- the Financial Services and Markets Act 2000 (as amended);
- the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001; and
- the Consumer Credit Act 1974 (as amended).

Together these regulate B2C credit terms, including any form of 'financial accommodation', and specify certain contract terms and restrictions (including sanctions, including legal unenforceability except by court order), the provision of certain kinds of information, the format of that information, cooling-off periods, and termination processes.

The above are not exhaustive lists.

The CMA, the UK's primary competition and consumer authority, has historically taken a close interest in B2C cloud storage contracts, in particular to see if consumers are being fairly treated when saving and storing their content online. The CMA was concerned that some CSPs were using contract terms and practices that could breach consumer protection law ('An open letter to cloud storage providers on complying with consumer law', May 2016). The upshot was that several of the leading B2C cloud storage providers, including Amazon, Apple and Microsoft, voluntarily modified their terms for the benefit of UK consumers. You can find a list of all of the consumer outcomes secured by the CMA and relating to Cloud Storage here.

Following the end of the transition period, we are starting to see UK and EU consumer regimes diverge, which will have an impact on UK traders selling to EU consumers. The United Kingdom has now revoked the Consumer Protection Cooperation Regulation (the CPC Regulation) which facilitates co-operation between EU enforcement authorities. UK consumers are also no longer able to use the EU's online dispute resolution platform to resolve disputes arising from cross-border B2C transactions with the help of an approved dispute resolution body. However, certain amendments made as a result of the CPC Regulation to English law (and which have been retained) grant enforcement authorities greater powers to intervene in the digital sphere. So the CMA has a new power to apply to the High Court for an online interface order or an interim online interface order where the CMA believes there has been an infringement of consumer law in the UK. Also, significant changes are to be made to EU consumer law as a result of the transposition of three significant EU directives in 2021 and 2022: the Digital Content and Digital Services Directive (2019/770) and the Sale of Goods Directive (2019/771) both of which had a transposition date of 1 July 2021; and the Enforcement and Modernisation Directive (2019/2161), which is to be transposed into national law by 28 November 2021.

While the United Kingdom is not required to implement these latest EU directives, UK traders selling to EU consumers will still be affected by the new rules, which impose more stringent penalties for non-compliance with consumer protection law, with fines linked to turnover. At the time of writing, the United Kingdom has indicated that it is likely to adopt similar enforcement measures and penalties in English law (when legislative time allows). The recent Penrose report that examined the UK's competition and consumer regimes identified three areas of suggested focus for stronger consumer protection:

- loyalty penalties and price discrimination;
- unfair terms hidden in long or complex consumer contracts; and
- commercial practices 'nudging' consumers (eg, poorly explained subscription deals, hidden opt-outs for added costs, creating urgency around price or availability, or using default settings to influence consumer behaviour).

The Penrose report was followed by a report by the Taskforce on Innovation, Growth and Regulatory Reform's May 2021 report setting out proposals for a new post-Brexit regulatory framework for the UK (focusing on outcomes-based, proportionate regulation). This report specifically mentioned cloud services in the context of fintech and noted that the UK needs to ensure the policy and regulatory approach continues to protect consumers while creating an enabling environment that encourages growth and competition.

Changes proposed to the UK data protection regime and proposals relevant to fintech and digital health may be relevant to cloud service providers.

Sector-specific legislation

13 | Describe any sector-specific legislation or regulation that applies to cloud computing transactions in your jurisdiction.

The extent (if any) to which UK industry sectoral regulation may apply to cloud computing will require knowledge and examination of sector-specific legislation, regulations, guidance and regulatory and statutory codes of conduct. In the United Kingdom, with the exception of the NIS Regulations and the following example, at the time of writing, there is no regulation that applies specifically or directly to cloud computing as such. Where regulation is found to apply to a cloud computing project, the approval, licence or consent – or at least the informal go-ahead – of a regulator may be required. Common sense and best practice dictate that, where applicable, the regulated entity should consult its regulator as soon as practicable and as fully as possible. This should also be of concern to a CSP expecting to enter a cloud arrangement with a regulated customer.

UK financial services

Only in the UK financial services sector has cloud computing been specifically addressed. Operational resilience, including outsourcing to the cloud, has long been identified as a cross-sector priority in the Financial Conduct Authority (FCA)'s annual regulatory business plans. Building on an FCA, Bank of England and Prudential Regulation Authority (PRA) paper (DP 18/4), in December 2019 the FCA, Bank of England and PRA published a shared policy summary and coordinated consultation papers on new requirements to strengthen operational resilience in the financial services sector: FCA CP19/32 and PRA CP19/29. The FCA's CP19/32 contains a chapter on outsourcing, which includes cloud computing; in March 2021, the Bank of England, PRA and FCA released shared policy statement 21/3, setting out the consultation feedback and their joint response to it. The PRA's CP19/29 was followed by the PRA's supervisory statement 6/21 which provides feedback on the consultation and contains the PRA's final policy. CP 19/29 was accompanied by CP 30/19, 'Outsourcing and third-party risk management'. The objectives of CP 30/19 were to deliver on the commitment to 'facilitate greater resilience and adoption of the cloud and other new technologies', as set out in the Bank of England's response to the Future of Finance report, and to support the proposals on operational resilience.

In March 2021, the PRA issued Supervisory Statement 2/21 (SS 2/21), setting out its expectations as to how PRA-regulated firms should manage outsourcing and third-party risk management generally, with the express aim of facilitating 'greater resilience and adoption of the cloud and other new technologies'. SS2/21 also reflects the European Banking Authority's (EBA) 'Guidelines on Outsourcing Arrangements' (EBA Outsourcing Guidelines). Separately, despite the end of the Brexit transition period, the FCA expects banks, building societies and certain investments firms to comply with the EBA Outsourcing Guidelines,

which replaced earlier guidance from 2006, and incorporated the EBA Recommendations on Outsourcing to Cloud Service Providers, which were applicable from 1 July 2018. Prior to the finalisation of the EBA Outsourcing Guidelines and SS2/21, the FCA had already issued what is known as Finalised Guidance: FG16/5 'Guidance for firms outsourcing to the "cloud" and other third-party IT services' (FCA Cloud Guidance). First published in July 2016, this has since been updated to reflect that while it remains applicable to some regulated entities, firms subject to the now finalised EBA Outsourcing Guidelines do not need to also follow the FCA Cloud Guidance.

Broader regulatory context

Before outlining the EBA Outsourcing Guidelines, SS2/21 and the FCA Cloud Guidance in more detail, they must be put in their sectoral regulatory context. When financial services organisations regulated under the Financial Services and Markets Act 2000 (as amended) by the FCA and PRA engage in any IT, business process or other outsourcing, they must have regard to and, if applicable, comply with, the regulatory guidance and rules governing that outsourcing. The PRA supervises banks, insurance companies, building societies, credit unions and certain large investment entities. The FCA regulates the business conduct of all financial services organisations within its statutory jurisdiction, including those prudentially supervised by the PRA. Some outsource providers (which are also CSPs) are themselves authorised and regulated by the FCA. The FCA Handbook and PRA Rulebook are also relevant sources of rules and guidance.

The PRA and FCA rules are complex and their application to an outsourcing will depend on the nature of the firm (the outsourcing customer), the financial services and related activities to be outsourced and the impact of the proposed outsourcing. There are also specific outsourcing-related obligations on insurance and reinsurance companies under the Solvency II Directive (2009/138/EC) and related subordinate rules and guidelines, including, in particular, Commission Delegated Regulation (EU) 2015/35 supplementing Solvency II, and, for firms in other sectors, in the Markets in Financial Instruments Directive (MiFID) II (2014/65/ EU) and related subordinate rules and guidelines, including, in particular, Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II, as they form part of retained EU law in the UK. These are the main sources of prudential and operational provisions regulating outsourcing by financial services firms and regulated outsource providers in the UK.

The detailed rules governing outsourcing are beyond the scope of this section. In essence, though, the rules provide for what should be regarded as sensible outsourcing practice, having regard to concentrated and systemic risk, initial diligence and ongoing operational risk affecting the conduct of regulated business and the interests of business and consumer end customers, and the needs of the regulators to supervise and intervene if necessary. Different requirements and guidance apply to different types of firms and may also depend on the type of function being outsourced. For example, whether the function being outsourced is considered critical or important, is a material outsourcing, or involves important operational functions.

This section now briefly summarises the EBA Outsourcing Guidelines, SS2/21 and the FCA Cloud Guidance.

Overview of EBA Outsourcing Guidelines

The EBA Outsourcing Guidelines are divided into five sections or Titles:

1 Proportionality: group application and institutional protection schemes (setting out a principle of proportionality in application of the EBA Guidelines, and requiring transparency within groups);
2 Assessment of outsourcing arrangements (defining 'outsourcing' and 'critical or important' functions);
3 Governance framework;
4 Outsourcing process (setting out aspects to be included in an outsourcing agreement at a minimum for a critical or important function); and
5 Guidelines on outsourcing addressed to competent authorities.

The governance framework in Title III requires: a holistic risk management framework, a written outsourcing policy, management of conflicts, business continuity plans, internal audit and a register of information on all outsourcing agreements.

The outsourcing process under Title IV is split into several chapters, with the contractual requirements being contained in Chapter 13. Chapter 13 is further subdivided into the following sections:

1 Contractual phase;
2 Sub-outsourcing of critical or important functions;
3 Security of data and systems;
4 Access, information and audit rights; and
5 Termination rights.

The FCA has amended its guidance, so rather than requiring firms to amend existing outsourcing arrangements to comply with the EBA Outsourcing Guidelines by 31 December 2021, the new expectation is that firms should amend existing arrangements at the first appropriate contractual renewal or revision point. Where critical or important outsourcing arrangements have not been revised by 31 March 2022, firms are expected to notify the FCA.

Overview of SS2/21

SS2/21 applies to various types of firms, including banks, building societies, PRA-designated investment firms, UK Solvency II insurers and UK branches of overseas insurers. It focuses on data security, audit, sub-outsourcing, and business continuity and exit plans, as well as including a list of provisions the PRA requires outsourcing contracts and material outsourcing contracts to include.

It also sets out requirements for pre-contractual due diligence and internal governance relating to material outsourcings and obliges firms to implement proportionate and risk-based controls for non-outsourcing third-party arrangements that are material or high-risk.

SS2/21 is largely based upon the EBA Outsourcing Guidelines. As well as containing various guidance for regulated firms on how they should consider and manage their outsourcings, SS2/21 provides further details as to what the PRA expects firms to include in their outsourcing contracts. In this regard, SS2/21 largely follows the same categorisation as the EBA Guidelines and provides additional detail on business continuity and exit strategies.

The PRA requires material outsourcing agreements entered into on or after 31 March 2021 to be compliant with SS2/21 by 31 March 2022. Any 'legacy' agreements entered into prior to 31 March 2021 need to be updated at the first appropriate contractual renewal or revision point, to meet expectations 'as soon as possible' after 31 March 2022.

Overview of the FCA Cloud Guidance

The FCA Cloud Guidance is addressed to those firms to which the EBA Outsourcing Guidelines do not apply 'when outsourcing to the "cloud" and other third-party IT services'. As is evident from the FCA Cloud Guidance, for the FCA, cloud computing is not only equivalent to outsourcing in its potential impact on regulated firms, their operations and end customers, but also it sees the cloud 'as encompassing a range of IT services provided in various formats over the Internet' (paragraph 1.4 FCA Cloud Guidance). Accordingly, the FCA sees no distinction between the use of private, public or hybrid cloud, IaaS, PaaS or SaaS.

The stated aim of the FCA Cloud Guidance is to facilitate the adoption of cloud computing in the regulated financial services sector, recognising the benefits of cloud computing and innovation in the

sector. It came about because firms and CSPs had told the FCA that they were unsure about how to apply its Handbook outsourcing rules to the cloud: this uncertainty may have been acting 'as a barrier to firms using the cloud' (paragraph 1.3 FCA Cloud Guidance).

UK Finance – public cloud computing framework

The UK banking sector trade body, UK Finance, sponsored the creation of a public cloud computing framework in February 2019. The framework consists of 44 controls, with each control mapped to one of nine domains and one of 11 risks associated with the management of cloud computing as a service. The controls are derived from analysis of UK Finance members' control sets and in collaboration with CSPs, cross-checked for compliance against various industry standards as well as the EBA Guidelines. Despite laudable efforts by the regulators and industry bodies to help firms around financial services regulatory hurdles in adopting the cloud, there are still significant concerns about the compatibility of cloud computing with regulatory compliance.

Insolvency laws

14 | Outline the insolvency laws that apply generally or specifically in relation to cloud computing.

There is no specialist insolvency regime for cloud computing. The primary UK insolvency regime is set out in the Insolvency Act 1986 and the Insolvency (England and Wales) Rules 2016 (both as amended). PwC's Business Recovery Services has produced a guide to the UK insolvency regime.

The rules that govern the insolvency of a CSP or a cloud customer, as well as those governing how corporate insolvencies are managed and disposed of, are complex. Experience in the UK has shown just how difficult it can be for cloud customers when a CSP suffers financial distress and insolvency. In early 2013, UK CSP 2e2 went into administration and subsequently liquidation. As a result, UK CSP customers are advised to consider carefully:

- the selection of their CSP;
- ongoing monitoring of the financial robustness of the CSP; and
- the terms of their cloud service contracts, including:
  - ownership of the customer's tangible and intangible assets;
  - exit arrangements; and
  - data migration where the CSP suffers financial distress or insolvency.

In addition, CSPs and other IT providers operating in the UK need to be aware of legislation that could severely restrict their ability to withdraw service from insolvent customers, terminate supply contracts or demand higher payments for continuity of supply. The legislation overrides conflicting terms in a supply contract (see sections 233 and 233A of the Insolvency Act 1986 (as amended by the Insolvency (Protection of Essential Supplies) Order 2015)). The amendments introduced by the 2015 Order ensure that, like utility services, 'communication services' and other IT supplies are treated as essential supplies. 'IT supplies' include a 'supply of goods and services [. . .] for the purpose of enabling or facilitating anything to be done by electronic means', specifically including computer hardware and software; information, advice and technical assistance in connection with the use of information technology; data storage and processing; and website hosting – in other words, they are wide enough to cover cloud computing services.

The regime prevents suppliers of 'essential supplies' (ie, water, electricity, gas, communication services and other IT supplies) from requiring payment of pre-insolvency charges as a condition of continuing to provide supplies in specified formal insolvency situations. In addition, where a customer enters either administration or a company voluntary arrangement, the regime locks the CSP into the pre-insolvency contract (subject to certain safeguards) to prevent the CSP from terminating supply, terminating the contract or increasing prices. However, the protections for customers of essential supplies do not apply to contracts for the supply of goods and services where either the company or the supplier is involved in financial services (which include situations where the company or supplier is an insurer, bank, electronic money institution, investment bank or investment firm, payment institution, operator of payment systems or a recognised investment exchange). In practice, this means that financial services firms and their creditors or suppliers can continue to terminate contracts, as they see fit.

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

15 | Identify the principal data protection or privacy legislation applicable to cloud computing in your jurisdiction.

The main data protection and privacy legislation in the UK comprise of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The UK's data protection regime remains substantially aligned to that of the European Union following the expiry of the transition period on 31 December 2020; however, some divergence is likely to occur over time. The Data Protection Act 2018 is the successor of the Data Protection Act 1998. It supplements, and must be read alongside, the UK GDPR. The Information Commissioner's Office (ICO) issued, for organisations rather than members of the public, specific guidance on the use of cloud computing. Although this guidance has not yet been updated to reflect the UK GDPR and Data Protection Act 2018, the ICO states that it 'still considers the information useful'. Based on previous statements made by the ICO, it is expected that the guidance will be updated soon.

The following section outlines the likely and most direct impact on cloud computing in the UK of the UK GDPR and the Data Protection Act 2018.

General knowledge of the principles of the UK GDPR and the terminology used in that legislation is assumed. It is beyond the scope of this section fully to cover the contents and operation of the UK GDPR. The following focuses on certain elements of the UK GDPR that are new to data protection law or that have particular significance for cloud computing. This outline is not, therefore, exhaustive. References below to articles are to the articles of the UK GDPR. Where we refer to 'GDPR' this means the UK GDPR and the EU GDPR collectively.

Territorial scope

The territorial scope of the UK GDPR is modelled on that of the EU GDPR. It follows then that the UK GDPR applies to the processing of personal data within the context of the activities of an establishment of a controller or processor in the UK, regardless of whether such processing takes place in the UK or not. Clearly, the UK GDPR applies to the processing of personal data of a controller or processor in the UK; in addition, guidelines on territorial scope issued by the European Data Protection Board (EDPB) indicate that 'within the context of the activities' is capable of a wider meaning depending on the context itself. This developing area will be of interest to CSPs.

The UK GDPR will also apply to the processing of personal data of data subjects in the UK by data controllers and processors with no UK establishment where the processing relates to offering goods and services (free or for payment) to UK data subjects, or to monitoring the behaviour taking place in the UK of such data subjects (article 3(2)). The UK GDPR may, therefore, apply to CSPs (assuming them to be either processors or controllers) without sites in the UK, if they meet either or both of the above tests. Certain controllers or processors (including CSPs) will have to appoint a local UK representative for legal enforcement purposes (article 27).

Data controllers

Generally, though it should not always be assumed, in B2B cloud computing the customer will be the controller of any hosted personal data, as the customer will be determining the purposes and means of the processing of such personal data (article 4(7)). This characterisation continues under the UK GDPR and this is to the advantage of CSPs as, ultimately, the controller will be bound by more stringent duties than the processor. One area where this relationship could be open to question is if a CSP was looking to contract on the basis of its standard public cloud terms with customers who are consumers. The UK GDPR does not apply to processing done wholly for domestic or household purposes, so consumer customers could be neither controllers nor processors, indicating that such standard terms could be a poor fit.

The controller, or cloud customer, will be primarily liable for identifying a lawful basis for processing, as well as implementing appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing is performed in accordance with the GDPR, including ongoing reviews and the updating of those measures (article 24(1)). Cloud customer-controllers must, therefore, be able to demonstrate that processing performed on their behalf by CSPs is compliant, which in turn will mean having to satisfy themselves that CSP contract terms facilitate the controller's obligations.

Controllers should only engage processors who provide sufficient 'guarantees' to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of the GDPR and ensure the rights of data subjects (article 28(1)). This raises important questions for cloud customer due diligence in appointing CSPs. In some cases, this aspect of the decision will almost certainly have to be documented (eg, regulated financial services firms deciding to engage CSPs for their operations).

The controller may refer to the adherence to approved codes of conduct under article 40 or to approved certification mechanisms under article 42 for the purpose of demonstrating compliance with its UK GDPR obligations (the current EU Agency for Network and Information Security framework is available online). We can expect to see further development by CSP industry organisations of cloud-specific codes of conduct and certification mechanisms in the coming years. May 2021 saw the EDPB and the Belgian Data Protection Authority approve the EU Cloud Code of Conduct. The Code is applicable to all cloud service provision models. It will apply in circumstances where a CSP acts as a processor of personal data in line with article 28 of the GDPR. In addition, the EDPB and the French Data Protection Authority recently approved the CISPE Data Protection Code of Conduct for Cloud Infrastructure Providers in Europe, which is applicable to infrastructure as a service cloud offering.

Although article 28 is headed 'Processor', it is clear that some of the obligations it imposes, for example, under article 28(1), are directed to and will be the primary responsibility of controllers. So it is with article 28(3), which requires not only for there to be a binding contract between the controller and processor governing data processing, but also for that contract to stipulate a range of specific provisions (article 28(3)(a)-(h)), including, for example:

- that processing will only be in accordance with the controller's documented instructions, including with regard to third-country data transfers;
- confidentiality undertakings by all those authorised to process the data;
- controls on the engagement of sub-processors; and
- processor obligations to assist the controller in ensuring compliance under articles 32 to 36 regarding its obligations of data security, pseudonymisation and encryption, data breaches and notifications, and data protection impact assessments.

Cloud customers and CSPs must address these requirements in their cloud computing contracts, whether on the CSP's standard contract terms or otherwise.

Article 28(8) provides that both regulators and the European Commission may adopt standard contractual clauses (SCCs) covering the requirements of article 28(3): no such clauses have been adopted by the Information Commissioner's Office to date. On 4 June 2021, the European Commission published model article 28 clauses for voluntary use (further discussion is outside the scope of this chapter). We should expect that any SCCs adopted will be focused on compliance with the legislation's requirements, and may not be suitable for CSPs or customers wishing to accommodate commercial issues in their drafting.

Processors

As stated above, in B2B cloud computing, a CSP is usually likely to be – and to prefer to be – the entity processing personal data on behalf of the controller, namely the processor: article 4(8). Among the changes to data protection law made by the GDPR (and reflected in the UK GDPR) is that processors, hence CSPs, are for the first time directly accountable for and liable to data subjects and regulators for infringements. Aside from the need for a binding contract between the controller and processor with its various contractual stipulations, additional requirements imposed on processors include the following.

Processors must not engage sub-processors without the controller's prior specific or general written authorisation, including changes to sub-processors after general written authorisation has been given – so giving the controller the opportunity to object to those changes (article 28(2)). This could clearly have a material impact on cloud supply chains and changes to them. Moreover, where a processor has engaged sub-processors, it must impose by contract the same data protection requirements on those sub-processors as apply in the controller-processor head contract, in particular, to ensure that sub-processors provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the UK GDPR. Processors will be liable to controllers for the acts and omissions of sub-processors (article 28(4)).

Processors must keep a written or electronic record of all categories of processing activities undertaken for a controller (article 30(2)). There is an exemption for organisations employing fewer than 250 employees, with certain exceptions (article 30(5)).

There is a specific requirement for processors to cooperate with data protection supervisory authorities (article 31).

Another new set of obligations on processors relates to data security and breach reporting. In their own right, processors must – having regard to the state of the art, costs, risk, etc – implement appropriate technical and organisational measures to ensure:

- data security, including the pseudonymisation and encryption of personal data; and
- the confidentiality, integrity, availability and resilience of processing systems and services;
- the restoration and availability of data following 'physical or technical' incidents; and regular security testing (article 32(1)).

The economics of cloud computing – especially in public cloud deployment models – are likely to be challenged by these requirements.

Under article 33(2), the processor must notify the controller 'without undue delay' after becoming aware of a personal data breach. This must be seen in the context of the controller's new obligation to notify its supervisory authority – except for breaches unlikely to compromise data subjects' rights – without undue delay and, where feasible, not later than 72 hours after becoming aware of a data breach, including details surrounding the breach (article 33(1) and (3)). CSP processors are often therefore required to support B2B customer controllers in

breach management and notification, which will, in turn, need to be reflected in cloud arrangements and contracts.

Sanctions and remedies

Under the UK GDPR controllers and processors will be directly accountable and liable for non-compliance, both to data subjects and regulators. The allocation of responsibility and liability for infringements between cloud customers and CSPs has, therefore, assumed even greater importance in B2C and B2B-related cloud contracts – particularly because of the extent and scale of the UK GDPR sanctions and remedies.

Any person who has suffered 'material or non-material' damage as a result of an infringement will have a right to receive compensation from the controller or processor (article 82(1)). Controllers will remain liable overall for such damage, while processors will only be liable where they have not complied with the GDPR obligations specifically directed to them or where they have acted outside or contrary to the lawful instructions of controllers (article 82(2)). A controller or processor that has paid full compensation to a data subject following a claim for damages is entitled to recover that element of the damage that they are not responsible for from the other controllers or processors involved in processing (article 82(5)).

Administrative fines will depend on the gravity of the non-compliance (article 83(2) (a)-(k), 83(3)). There are two tiers of fine for specified infringements: a lower level of up to £8.75 million or, in the case of businesses, up to 2 per cent of the preceding financial year's worldwide annual turnover, whichever is higher (article 83(4)); and an upper level of up to £17.5 million or, in the case of businesses, up to 4 per cent of the preceding financial year's worldwide annual turnover, whichever is higher (article 83(5)).

There are other processes and sanctions available for non-compliance under both the UK GDPR and the Data Protection Act 2018, including audits, access rights, reprimands and administrative orders (article 58).

Cross-border data transfers

These rules are dealt with in articles 44 to 50. As applied to cloud computing and cloud supply chains, they are an important part of the UK GDPR's regulation. Personal data transfers to recipients in 'third countries' continue to be closely regulated, broadly to ensure that the level of data protection for data subjects is not undermined (article 44). Overall, the UK GDPR framework for such transfers is closely similar to that under the EU GDPR and similar to that under the previous Data Protection Act 1998 and the EU Data Protection Directive (Directive 95/46/EC), with some new (although as yet unavailable) compliance measures, including the ability of data exporters to demonstrate compliance through approved codes of conduct and approved certification mechanisms (article 46(2)). Breach of these provisions will be a non-compliance issue for which the upper tier of administrative fines can be imposed. Both controllers and processors will be liable to non-compliance proceedings.

The Court of Justice of the European Union's (CJEU) judgment in the *Schrems II* litigation (*Facebook Ireland v Schrems* (Case C-311/18)) has created significant uncertainty for controllers and processors carrying out cross-border data transfers. While the SCCs (also known as 'model clauses') approved by the European Commission survived an invalidity challenge in July 2020, the CJEU stated that data exporters and data importers looking to rely on them must also consider the 'relevant aspects of the legal system' of the destination country. These aspects must be considered by the parties when assessing whether the level of protection offered in the case of any transfer to a third country (not just those to the United States) is 'essentially equivalent' to that guaranteed in the European Union. At the time of writing, guidance is awaited from the ICO on how such an assessment may be carried out and what further measures data exporters and data importers may be required to take. The EDPB issued guidance, which was finalised on 18 June 2021 (following the end of the Brexit transition period on 31 December 2020) on the measures which can be taken in order to supplement the EU GDPR's transfer tools in order to ensure an essentially equivalent level of protection over personal data to that guaranteed under the EU GDPR. Current guidance from the ICO on international transfers refers back to the EDPB's recommendations and states that the ICO will produce its own guidance on this topic in due course.

It is increasingly problematic for cloud customers and CSPs that there are no 'processor to processor' SCCs authorised for use in the UK. The European Commission approved a set of 'processor to processor' SCCs in June 2021 for use for EU outbound transfers of personal data.

UK's Adequacy Decision from the European Commission

On 28 June, the European Commission adopted its Adequacy Decision for the UK, putting to an end (at least for now), the uncertainty surrounding personal data flows between the European Union and the United Kingdom.

The Adequacy Decision means that personal data can continue to flow from the European Union to the United Kingdom, on the basis that the latter currently guarantees an essentially equivalent level of protection to that provided under EU law. This avoids the need for EU exporters to satisfy the restrictions in the EU GDPR, such as entering into SCCs with the UK entity importing the data. Unusually, and for the first time, this Adequacy Decision includes a sunset clause, requiring it to be renewed after four years. This is different from the re-assessment approach taken with earlier country adequacy decisions.

It is likely that this was included in recognition of concerns expressed by the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs about the current (and possible future) adequacy of the UK's data protection regime, centred on the UK's bulk data collection practices.

Another challenge for the EU was addressing the potential for the UK to diverge from EU norms in the future. Now it has been granted, the European Commission will continue to monitor relevant developments in UK law to confirm that adequate standards of protection are maintained, failing which, the Adequacy Decision can be suspended or repealed in whole or part, even before the expiry of the initial four year period.

Privacy Shield following Schrems II

Adopted in July 2016, the EU-US Privacy Shield applies to EU-US data transfers and is therefore relevant for cloud computing in EU-US and related trade. Microsoft claimed to be the first US CSP to appear on the US Department of Commerce's list of Privacy Shield certified entities. However, following the CJEU's July 2020 decision in *Schrems II*, the Privacy Shield is no longer valid as a legal mechanism for companies in the European Union sending personal data to Privacy Shield program members in the United States. This has significant ramifications for cloud service providers that rely on the Privacy Shield mechanism for EU-US data transfers.

Access to EU personal data by third-country governments

In the light of the Snowden disclosures and the litigation that followed (eg, *Microsoft v United States*, No. 14-2985 (2d Cir. 2016), it is worth noting that article 48 of the GDPR contains specific safeguards against governments of third countries accessing EU personal data. Any third-country judgment or administrative decision requiring a controller or processor to disclose EU personal data will only be enforceable if it is based on an international agreement (eg, a mutual assistance treaty between that third country and the European Union or a member state).

(See the Agreement on Mutual Legal Assistance between the US and the EU, signed 25 June 2003.)

CLOUD COMPUTING CONTRACTS

Types of contract

16 What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

In the United Kingdom, contracts cover the full range of cloud service and deployment models and reflect the country's large and sophisticated cloud business ecosystem, including cloud service provider (CSPs) supply chains.

One aspect of cloud contracting that tends to cause difficulties for cloud customers is where, as is typical, cloud contract formats are modular. This means that the provisions of the contract must be located from a combination of offline and online sets of terms or, more typically, from a combination of multiple online sets of terms, policies, etc, which users must access by clicking on different hypertext links. These sets of terms are then assembled and stipulated by the CSP to form the entire contract.

The European Commission Study on consumers' attitudes towards Terms and Conditions published in 2016, which looked at typical consumer reading times of terms and conditions (T&Cs), which indicated reading times of around two minutes for lengthy T&Cs and slightly more than 30 seconds for shorter T&Cs, and showed that despite readership of the T&Cs being very low, the vast majority of consumers do accept the T&Cs when required to indicate acceptance when concluding a transaction. This is supported by the findings of an earlier US study, which found (in a study of 50,000 visitors to 90 software company websites) that only around 0.2 per cent of online customers accessed a product's end user licence agreement (EULA), spending, on average, under a minute on a EULA page (Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' NYU Law and Economics Research paper No. 09 – 40 (2009). In 'Contracts for Clouds, Revisited: An analysis of the standard contracts for 40 cloud computing services' by Johan David Michels, Christopher Millard and Felicity Turton (Queen Mary University of London, School of Law Legal Studies Research Paper No. 334/2020) (Queen Mary Cloud Study), the authors noted that the terms of service surveyed were lengthy, consisting of documents incorporated by reference, using the example of Facebook's terms of service documents, which combined amount to more than 33,000 words, which would take a typical adult over two hours to read. In our experience, these formats and contract processes make it difficult even for sophisticated corporate customers to ascertain the full extent of cloud contracts and, in some cases, to determine what terms will govern them. In B2C contracts, and possibly where B2B cloud customers are negotiating on CSP standard terms of business, this difficulty in ascertaining applicable contractual terms could, in certain circumstances, ultimately result in the legal ineffectiveness or unenforceability of certain contract terms and lead to regulatory intervention. A 2020 English case looking at the enforceability of online terms (*Andrew Green v Petfre (Gibraltar) Lt t/a Betfred* 2020) made clear the risks of relying on lengthy, overlapping and inconsistent terms in the B2C context – the exclusions clauses were held not have been properly brought to the attention of the consumer, with the effect that they were not incorporated into the contract. The judge also held that the clauses were unfair under the Consumer Rights Act 2015, and would therefore have been unenforceable.

The answers to the next six questions are based on a review and knowledge of a limited, but meaningful, range of B2B public cloud service agreements (CSAs) and related documents proposed by the major international CSPs that are available from public resources; and commentary in the June 2020 Queen Mary Cloud Study on a range of CSPs' terms of service. It is beyond the scope of this work to survey a much wider range of such contracts or to segment them by deployment model, service model or specific cloud services within each service model. Readers are referred to the work of leading UK academics (including *Cloud Computing Law*, Christopher Millard (ed), (Oxford University Press 2013) and the Queen Mary Cloud Study), noting that, inevitably there will have been changes to CSA practice and that we expect practices to continue to change in respect of the United Kingdom now that the Brexit transition period has ended. We also wish to acknowledge the excellent reports and other deliverables produced by the (now decommissioned) SLALOM Project teams. SLALOM documentation is recommended reading for this area and may be downloaded from the European Commission's website, using 'slalom' as a search term.

The answers below do not identify CSPs by name; they reflect a composite, high-level, view of the CSAs and related materials reviewed. Moreover, they do not attempt to assess the reasonableness, fairness or validity of the terms outlined. Here, we adopt the approach taken by the SLALOM Project team: readers will be aware that, in assessing these matters, much will depend on the context of the service and deployment and service model or models adopted, the relative bargaining strength of the parties, the economic basis of the cloud arrangement, cost or no-cost, and whether it is a beta product or service, etc.

Following the conclusion of the UK–EU Trade and Cooperation Agreement, and given the lack of mutual recognition arrangements for regulated sectors, UK-based CSPs offering services in the European Union will need to track EU-wide developments in this sphere, to ensure compliance with EU guidance. The European Commission actively promotes the development and use of fair standard cloud computing contracts and standardised service level agreements to guarantee the quality of cloud services in the European markets. Details of the initiatives currently being undertaken and revised by the European Commission include:

- launch of a European Alliance for Industrial Data, Edge and Cloud;
- joint investment in cross-border cloud infrastructures and services to build next-generation cloud supply (and to enable Common European Data Spaces);
- a European marketplace for cloud services, as a single point of entry to find certified cloud services; and
- an EU Cloud Rulebook for cloud services and infrastructures, which will provide clarity on the compliance of cloud services with relevant rules.

Finally, the role of international standards, such as ISO/IEC JTC1 SC38 for cloud computing and distributed platforms, will be ever-more important as applied to cloud computing services, service level agreements (SLAs) and CSAs.

Typical terms for governing law

17 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

With limited exceptions, the governing law of the CSP's home jurisdiction or a chosen regional location will apply. For certain purposes, for example, EU data protection standard contractual clauses (SCCs) will mean that the choice of governing law and jurisdiction may be those of the customer's location (although the new EU SCCs envisage that parties in some circumstances be able to select the governing law and choice of jurisdiction of any EU member state, such as when the EU SCCs are to cover multiple originating country transfers). Courts (rather than arbitral tribunals) competent in the CSP's jurisdiction

are most commonly chosen, with just less than a quarter of CSPs surveyed opting for binding arbitration clauses (Queen Mary Cloud Study). US CSPs usually require all customers to commit to compliance with applicable US export controls, sanctions and related laws and regulations.

The Queen Mary Cloud Study indicates that of the 40 CSP terms of service (ToS) surveyed, around half were governed by English or Irish law (in respect of English contracting parties, although this is based on the authors identifying the law applicable to consumers in the United Kingdom, where the ToS provided for differing choices of law depending on the identity of the customer), with the remainder governed by the law of a US state, Luxembourg or Switzerland.

Following the United Kingdom's withdrawal from the European Union, it may be that UK-based CSPs making agreements with EU entities give extra consideration to the provisions which are most appropriate for jurisdiction and enforcement, although changes to clauses are probably only likely where a CSP identifies a particular local law issue in a relevant member state. We have already seen Alphabet change Google's contracting entity for UK customers from an Ireland-based entity to Google LLC, which is registered in the US, and change the governing law to Californian law, which it ascribes to the United Kingdom leaving the European Union. VMWare has also recently updated its ToS so that the governing law is now the 'laws of Ireland' if the billing address is outside the United States (and the laws of the state of California and the federal laws of the United States, if the billing address is in the United States). No other major CSPs have altered their jurisdiction provisions following the end of the Brexit transition period on 31 December 2020. It remains likely UK-based business customers may see (depending on post-Brexit changes to the data protection regime in the UK following the grant of the UK's adequacy decision) more non-UK CSPs opting to contract through non-EU entities using US governing law and jurisdiction clauses. This would have an impact on UK customers' ability to seek redress for breach of the terms of service.

Typical terms of service

18 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

Pricing and payment

Pricing will, of course, vary depending on the deployment and service model offered, and whether the contract is formed online or offline. Some CSPs reserve the right to vary charges for existing services. There are usually remedies for late payment, including interest and, in some cases, the right for the CSP to suspend service for payment defaults. If the customer defaults on payment when due, all CSAs reviewed entitle the CSP to terminate them.

Suspension of service by the CSP

It is common to see suspension rights in addition to specific termination rights (and sometimes for the same or overlapping triggering events). The most typical cause for suspension is where there has been a breach by the customer or an end-user of the acceptable use policy (AUP), which will usually include the customer or an end-user causing security risks to the cloud service, the CSP or other cloud service users, or infringing third-party rights or failing to pay or entering insolvency proceedings.

Suspension may be on notice or, where urgent (as in the case of security risks), without notice. In some cases, the customer will remain liable to pay the charges during the suspension period, while service credits will not accrue.

Acceptable use policies

The CSAs of all the major CSPs contain an AUP: it has become one of the defining features of CSAs in the United Kingdom and elsewhere. Readers will be familiar with the standard terms of AUPs, which address conduct by both customers and their end-users in using the cloud services, and will include prohibitions on:

- illegal activities of any kind;
- violation of any third-party rights (including reverse engineering of the service) or conduct that violates any applicable law;
- gaining or attempting to gain unauthorised access to any networks, systems, devices or data;
- unauthorised disruption of any networks, systems, devices or data;
- sending unsolicited messages or marketing; and
- distributing malware.

There are also typically restrictions on the type of customer who can use the services (by age limit) and the purpose for which the service can be used.

Breach of the AUP may entitle the CSP to suspend or terminate the CSA – in some cases, a breach by a single end-user could result in suspension or termination. Other CSAs contain indemnities for AUP breaches. Where the AUP has been breached, or the CSP suspects the breach was due to illegal conduct, the CSP may report those activities to the authorities or interested third parties and reserve the right to cooperate with them.

Variation

One of the more disquieting terms of CSAs in the United Kingdom and elsewhere is that CSPs may, without the customer's consent, vary cloud services, SLAs and other terms of the CSA, usually without any justification and, in some cases, without the obligation to notify customers beforehand. (However, it is becoming more common for the CSPs to include a notice period for at least some types of changes to the terms. This is usually done by posting a revised version on a website, by emailing the customer or through a notification in the user interface, and customers who continued to use the service are deemed to have accepted the new terms.) Some standard ToS now expressly permit a customer to terminate for variation of the terms of the CSA, although this places the burden on customers to monitor the ToS to identify when the terms vary and is burdensome for customers using a multi-cloud model.

A very small number of the ToS surveyed in the Queen Mary Cloud Study expressly stated that the CSP's contract terms would not vary during the contract period, providing a greater level of contractual certainty as to the applicable ToS. In B2C contracts, suppliers may only alter the terms of a contract of indeterminate duration unilaterally after providing the consumer with reasonable notice of the proposed variation (Consumer Rights Act 2015, Sch.2, 11, 23).

Typical terms covering data protection

19 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

To reflect the entry into force of the EU GDPR, all the major CSPs operating within, or providing services to, the European Economic Area introduced detailed data protection and processing terms for incorporation into their CSAs, in some cases in separate addenda or supplements. Where we use the terminology 'GDPR' this refers to both EU and UK GDPR.

Typically, the GDPR-related terms include:

- the allocation of processor and controller roles and functions between the customer and the CSP, with the CSP as processor and

with the right for the CSP to appoint sub-processors (subject to the customer's right to object to the appointment of new sub-processors and with concomitant sub-processor obligations);
- the application of technical and security features provided to the customer to enable it to comply with the technical and organisational measures required by the GDPR;
- deeming of 'documented' customer instructions to the CSP with regard to the CSP's processing of customer data in accordance with the GDPR;
- confidentiality obligations of the CSP in relation to customer data;
- terms for the handling of data subject access requests;
- detailed operational security provisions, including security breach notification obligations on the CSP;
- CSP data security certification and audits;
- provision for the transfer of personal data outside the United Kingdom or European Economic Area (as appropriate), with the incorporation of the SCCs accordingly;
- the return or deletion of customer data on termination of the CSA;
- obligations relating to record-keeping of all processing activities; and
- terms ensuring the processor's cooperation with the relevant regulator in the performance of their duties.

As of the time of writing, there have been no reported legal challenges emanating from the United Kingdom to CSP GDPR terms.

Typical terms covering liability

20 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

Liability

Understandably, all CSAs contain limitations and exclusions of liability: some are written from a US perspective, while others are localised. The CSP's liability is commonly limited (sometimes mutually) to the amount of charges paid by the customer – typically during the 12 months preceding the event giving rise to liability, with absolute caps ranging from US$20 to US$100,000. Liability caps of this kind are sometimes tiered by reference to different services (eg, the greater of a specified monetary amount or the total charges paid, depending on the service). In negotiated contracts, we generally see customers agreeing to a 'super cap' for CSP data protection breaches, rather than looking for unlimited data protection liability.

Some CSAs exclude from this limitation the CSP's liability for third-party intellectual property right infringements (whether under an indemnity or otherwise), and for confidentiality and data protection breaches.

It is common for CSAs to exclude liability:
- in general for direct and indirect, consequential, incidental, exemplary, punitive or special losses or damages (even if some of those kinds of loss or damages are not recognised in the UK jurisdictions and even if the possibility of such losses have been brought to the CSP's attention); and
- for a range of:
  - specific losses, including loss of revenue, loss of profits, loss of customers or goodwill, loss of use of data, loss of anticipated savings, loss of the use of the cloud service, etc;
  - causes (eg caused by breach of contract, inability to access a service, force majeure event or security breaches); and
  - theories of liability (eg, contract, tort or breach of statutory duty).

Not all of the broader contractual exclusion provisions will be binding under English law even for B2B contracts however, as where parties contract on standard form contracts that limit liability for breach of contract or for negligence, these clauses are required to be fair and reasonable in light of the circumstances at the time the contract was made (Unfair Contract Terms Act 1977, sections 2, 3, 11). Liability caps could also be the subject of challenge under Unfair Contract Terms Act 1977, depending on the context of the particular contractual relationship.

Some CSAs disclaim liability for unauthorised access to, and for the loss or destruction of, uploaded content and data. In other cases, CSAs will acknowledge the CSP's liability for content or data loss where the CSP has failed to meet its own security obligations. Many CSAs require customers to take responsibility for making backup copies of their own content and data or otherwise mitigating their own risks in using the cloud service.

Warranties and provision of service

Some CSAs contain a CSP warranty that it will deliver the services in accordance with the SLA or some other service description. Some CSAs state that cloud services are provided 'as is'. Almost invariably, any other express or implied warranties (eg, as to fitness for purpose, satisfactory quality, non-infringement) are disclaimed to the extent permitted by law. Some CSPs specifically exclude any express or implied warranty that the operation of the cloud service or software made available through it will be uninterrupted or error-free. The picture is slightly different in the consumer context, where CSPs will typically commit to providing the services with reasonable skill and care.

Indemnities

It is common for the customer to have to indemnify the CSP against the following actions by the customer and any end-user:
- any act or omission or use of the cloud service that infringes any third party's rights;
- breaches of the CSA generally and the AUP specifically;
- infringement of applicable law;
- creation or use of uploaded content; and
- in each case where the act, omission, use, etc give rise to claims, costs, losses etc.

Where there are detailed data processing provisions, including data transfer agreements, some CSAs will provide for customer indemnification of the CSP against breaches of data protection law caused by the customer or another end-user.

Service availability, quality, service levels and service credits

Many B2B public cloud CSAs contain or incorporate by reference specific SLAs as applicable to the service modules provided to the customer. For an example of CSA service levels applied by the major CSPs (and some others), readers should refer to the SLALOM Project's documentation.

While many CSAs provide that customers will not be entitled to claim for service unavailability for scheduled or unscheduled downtime or other service interruptions, we are seeing more CSPs offering SLAs in which they commit to deliver a certain level of service, and offer compensation to customers for failure to meet the SLA in the form of service credits. These are usually expressed as a percentage of the customer's monthly fees, usually set on a scale depending on the uptime percentage, thereby linking service credits to monthly spending, and usually capped at a percentage of a month's fees. Where service credits are included in an SLA, these are typically stated to be the customer's sole and exclusive remedy (which suggests the customer could not sue the provider for damages in relation to the service being unavailable). Some CSPs make specific claims or promises about their levels of service and are willing to enable the customer to terminate the CSA for stipulated breaches of those service levels, subject to following mandated procedures for doing so, with repayment of any prepaid charges. Many CSAs contain caps on the maximum amount of service credits allowable in a specified period.

The SLAs also require the customer to track downtime and make reports to claim service credits, with very few providers committed to proactively reporting on service availability levels. This would, of course, make monitoring and enforcing the SLA or service credit regime difficult for the customer. In other situations customers are required, within stipulated deadlines, to follow specified procedures to report service level breaches, as well as providing details of them for verification by the CSP, which may retain the option of rejecting a customer's claim. The SLAs also tend to exclude service unavailability where this arises from factors outside the CSP's control (eg, force majeure events, network or device failures outside the CSP's data centre, customer actions, third-party actions, the CSP system being down for maintenance or customer breach of the CSA or AUP). Customers will therefore usually need to accept the CSP's limited liability and factor this into the overall risk assessment of cloud service adoption (against the advantage of cost and scalability). To mitigate risks, customers may want to consider cyber insurance and resilience testing.

Business continuity and disaster recovery

In general, unless the CSP is providing a cloud-based business continuity service, CSAs do not contain any, or in any detail, business continuity or disaster recovery terms – although it is typical for CSAs to contain force majeure provisions excusing the CSP's performance in such cases. This is a feature of CSAs in the UK, US and elsewhere (see the useful report, Public Cloud Service Agreements: What to Expect and What to Negotiate Version 3.0 produced by the Cloud Standards Customer Council).

Usually, the customer is expected or obliged to make its own backup arrangements to ensure continuity. Sometimes, CSAs will refer to CSPs having their own disaster contingency plans for their data centres, using redundant processing and storage capacity to back up data held in those data centres, but without any contractually binding commitment to implement such plans.

Typical terms covering IP rights

21 | What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

The customer usually warrants that it owns or has all necessary rights to use its content (eg, software, data) processed by the cloud service or to grant any licences to the CSP under the CSA, and that its content or end-users' use of the customer's content will not breach the AUP (which may entitle the CSP to suspend or terminate the CSA) or that the customer will not use the services in any way which will or is likely to infringe third-party IP rights. Some CSAs require the customer to suspend access of an end-user to the service offering when the customer becomes aware of the end-user acting in violation of the obligations contained in the CSA. Some CSAs also contain an obligation requiring the customer to defend (and indemnify) the CSP against any third-party claim that the customer's content infringes third-party IP rights, and pay the amount of any adverse final judgment or settlement. For this to be effective in the consumer context, it would need to be appropriately flagged so as to be incorporated into the contract, so the consumer understands the consequences of the obligation it is undertaking.

The customer retains ownership of all IP rights in content uploaded or created by it in using the cloud service. The CSP is usually granted a limited licence to use the content to provide the cloud service (eg, covering rights of access, storage or distribution, as applicable) or to act on feedback, or to comply with regulatory or governmental directions or orders, and in some instances, the CSP's rights of use of the customer's content are extended to cover advertising.

The CSP may use without restriction any suggestions for improvements to the cloud service made by the customer, in some cases, with an obligation to assign the ownership in such suggestions to the CSP.

The CSP reserves rights in all IP rights relating to its cloud services, including IP rights in the applications and infrastructure used in providing the services. The scope of the licence granted to the customer to use the IP rights is typically very limited (ie, revocable, non-exclusive, non-sublicensable and non-transferable) and granted solely so that the customer can use the services. CSAs also typically include a prohibition on decompiling or reverse-engineering the services, or access and use of the services, to develop a competitive product.

If the cloud services are found, or understood by the CSP, to infringe any third-party IP rights, the CSP may at its discretion, and usually as a preferred remedy, procure the necessary rights for customers to continue using the services, modify the services so that they become non-infringing without any material loss of functionality, or provide equivalent services in substitution for the infringing services; or failing that, to terminate the part of the cloud services offering concerned (in some cases making an express commitment to refund a prorated portion of the fee paid). In some cases, instead of the above 'work around' language, the CSP will undertake to defend or indemnify the customer against the claims, costs, losses, etc, arising from final judgments. These are usually expressed to be the sole remedies available to the customer. The AWS terms also emphasise that AWS shall have no responsibility for the customer's use of third-party IP rights after it has notified a customer to discontinue such use and other CSAs make the customer's ability to claim under an indemnity subject to the customer notifying the CSP within a short specified time period. Where CSAs are governed by the laws of a US jurisdiction, customers may find that the obligation to defend does not include the obligation to indemnify – though this is, of course, to be determined under the relevant US jurisdiction if validly chosen.

In addition, where a CSP's offering comprises any open source software, this software will be made available to the customer under the terms of the applicable open source software licence. The VMWare terms of use enable a customer to obtain a copy of the licences and any source code (and modifications) that VMWare is required to make available under the open-source licences.

Typical terms covering termination

22 | What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

CSAs may allow termination for convenience on specified notice for both the customer and the CSP.

Either party will usually have a right to terminate for the material breach of the other, change of control of the other, or the insolvency of the other. There is often also a range of specific rights of termination by the CSP, including:

- Non-payment by the customer of due invoices. Note that the ability of a supplier to terminate a contract where the counterparty has entered an insolvency or restructuring process has been limited by the new measures introduced into the Insolvency Act 1986 in June 2020 (by the Corporate Insolvency and Governance Act 2020) which render these types of ipso facto termination clauses in goods and services contracts ineffective. However, the ban on these clauses does not apply in respect of contractual arrangements with insurers, banks, electronic money institutions and operators of payment systems and infrastructure providers.
- Where the cloud service is dependent on third-party IP rights (eg, software licences), when a relevant third-party licence expires or is terminated.

- For a specified period of customer inactivity.
- Where the customer or an end-user's use of the cloud service presents a security risk to the CSP or any third party (typically contained in the AUP).
- General discontinuance of the service by the CSP.
- Contravention of export and sanctions controls laws and regulations.
- One or more (other) breaches of the AUP or any other term of the CSA by the customer or an end-user.

A CSA containing a termination clause allowing a CSP to terminate a contract of indefinite duration with a consumer without reasonable notice is liable to be unfair under UK consumer protection law, which may mean a termination clause is unenforceable against a UK consumer.

The consequences of termination may include:

- the customer's obligation to cease using or to return any proprietary material (eg, software), or to destroy any content provided by the CSP;
- that the CSP will not erase the customer's data for a specified period after termination (unless otherwise required by law), and in some cases that the customer will be entitled to retrieve its data for a limited period following termination, prior to the data being deleted (usually also subject to a charge by the CSP);
- where the CSP has terminated for cause, that the customer must pay all unpaid charges for the remainder of the term; and
- where the customer has terminated for cause, that the CSP will refund any prepaid charges for the remainder of the term.

Employment law considerations

23 | Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

There are none that apply specifically to cloud computing.

However, depending on the cloud deployment model or service model adopted and the circumstances of the migration to cloud or the termination of the cloud service, cloud customers and CSPs should consider the application of the Transfer of Undertakings (Protection of Employment) Regulations 2006, as amended by (among others) the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 (together, TUPE). TUPE implements in the UK the EU Acquired Rights Directive 2001/23/EC.

In outsourcing transactions, because the application of TUPE is so well settled in the United Kingdom, it has become customary for the customer and outsourcing providers to provide, in a specific and detailed manner, for the legal, regulatory and financial implications of TUPE in the outsourcing contract, allocating duties, risk, costs and liabilities between them. In public and hybrid cloud contracts, the issue is often simply not considered and, therefore, is not provided for, most probably because the parties do not expect that TUPE will apply to such cloud arrangements or because CSPs that are based outside the European Union are unaware of the Acquired Rights Directive and TUPE.

However, neither CSPs nor their customers should assume that TUPE cannot or does not apply in relation to any of the cloud deployment models or service models. They should at least consider the question and take advice accordingly. The application of the Acquired Rights Directive and TUPE to, and their effect on, outsourcing are now widely understood in relation to the UK, where the government has expanded TUPE's application to outsourced services with the intention that TUPE should (if conditions are met) generally apply to outsourcing transactions. It is worth reiterating that TUPE is mandatory law: parties cannot disapply or contract out of TUPE.

In broad terms, where TUPE does apply, it transfers automatically by operation of law the staff from one organisation to another. Their terms and conditions of employment and continuity of service are preserved, and there are other procedural and substantive protections for the staff before and after a 'TUPE transfer' (eg, protection against dismissal and protection against changes to the transferring staff's terms and conditions of employment). There are also prescribed information (and in some cases, consultation) processes that must take place before any transfer. Accordingly, if TUPE applies to a cloud computing arrangement (in which one of the key drivers is cost-reduction) the potential financial implications resulting from the constraints and obligations arising out of TUPE may be significant and could undermine the economics of the arrangement.

In the UK, the most relevant trigger for TUPE in the context of cloud computing will be a 'service provision change' (rather than a 'traditional transfer' of an undertaking that retains its identity) where an in-house IT service ceases to be provided by the customer itself and is then provided by the CSP – or is migrated from one CSP to another CSP, or from the CSP back to the original customer if it wishes to resume the IT service in-house. This can constitute a service provision change under TUPE Regulation 3(1)(b). The workforce (organised grouping) carrying on the activities liable to transfer must be based in Great Britain and the principal purpose of that workforce must be to carry out those activities for the customer. In broad terms this means they must work wholly or mainly for the customer; although they may still do work for others (see TUPE Regulation 3(3), and the government's guidance on business transfers, takeovers and TUPE). More significantly for cloud computing arrangements, the activities to be carried out by the CSP must be 'fundamentally the same' as those previously undertaken by the customer's staff (see TUPE Regulation 3(2A).

So, the threshold question for a service provision change TUPE transfer in cloud computing migration is most likely to be: will the activities to be undertaken by the CSP be 'fundamentally the same as those undertaken previously by the customer's IT staff?' This will come down to an analysis of fact and degree. One – and only one – factor will be a reduction in the volume or scope of work, which is likely to be the case in a migration from traditional IT activities to the cloud (see *Department for Education v Huke and another* UKEAT/0080/12 and *OCS Group UK Ltd v Jones and another)*.

At first glance, IT activities or services migrated to, say, a public or hybrid cloud, from which the customer may then receive very different cloud services (at least by reference to the scope and possibly volume) to the services or activities previously provided in-house, simply do not intuitively look and feel 'fundamentally the same' in the cloud. And – if they addressed the question at all – it would be understandable if the customer and CSP considered that the activities to be carried out by the CSP are not 'fundamentally the same' as the original in-house IT activities so that TUPE would not apply. This could be a very costly mistake. In addition, there could still be a 'traditional transfer' of an undertaking that retains its identity under TUPE.

There will, of course, be other questions about which of the customer's staff members and how many of its IT workforce are in scope for TUPE, if it is likely to apply (see the government's guidance on business transfers, takeovers and TUPE).

It is worth reiterating that TUPE can apply equally to the subsequent move by the customer from one CSP to another, or back in-house to the customer, subject to the rules referred to above.

In cloud computing arrangements, it is quite likely that the CSP will be based outside the United Kingdom or that the cloud services will be provided from an offshore location. If there is an assigned workforce based in the United Kingdom, TUPE can apply to such arrangements, even if the service is provided from offshore. This is, however, likely to result in that assigned workforce becoming redundant.

TAXATION

Applicable tax rules

24 Outline the taxation rules that apply to the establishment and operation of cloud computing companies in your jurisdiction.

Consideration of the tax treatment of cloud computing will generally be more complex than in the case of terrestrial, in-country-only IT services. This is because tax authorities and businesses alike are grappling with the tax implications of cloud computing. The first step required is to correctly classify the underlying transaction to ascertain the correct tax treatment. Individual elements within the scope of and transactions comprising the cloud services will need to be analysed, in order to determine whether there is a transfer of property to the customer (ie, a sale, lease or licence of tangible property). If there is no such transfer then it is necessary to consider the tax rules in respect of the provision of services, assuming that the cloud services are properly characterised as services (eg, data processing, information service or a communications service). Consideration will also need to be given to the location of the cloud service provider (CSP) and its customers, to the source of the payments, and also to whether the location of the servers from which the services are provided can give rise to taxation.

The approach to taxation will also depend on the operating model of the supply chain of the cloud service; for example, whether it is intra-group or there are external providers in the supply chain and, if intra-group, whether the local CSP subsidiary performs sales and marketing functions for another group company or delivers the cloud services directly to local customers. See KPMG's guide to the taxation of the digitalised economy.

The following is a high-level outline of the UK taxes that are likely to be most relevant to cloud computing operations and the income derived from them. Both CSPs and cloud customers should seek specific advice on direct tax questions relating to UK cloud operations and service arrangements.

Corporation tax and permanent establishment

A company resident in the United Kingdom is subject to tax on the whole of its worldwide profits wherever they arise. A non-resident company is liable to corporation tax on profits attributable to a trade carried on in the United Kingdom through a permanent establishment (PE) in the United Kingdom. In determining whether a PE exists, the United Kingdom broadly adopts the OECD definition of PE (ie, 'a fixed place of business through which the business of an enterprise is wholly or partly carried on'). If a non-UK resident CSP has a fixed place of business in the United Kingdom through which some or all of its business is conducted, or has an agent acting on its behalf, it may be treated as having a PE in the United Kingdom and may be liable to UK corporation tax (currently 19 per cent).

In determining whether the presence of cloud servers in the United Kingdom leads to creation of a PE, HM Revenue & Customs' current approach is that the mere presence of a server or servers will not of itself create a PE. However, if the CSP is providing hosting services and the UK servers are essential for that hosting, this may result in the existence of a PE. Ultimately, whether a server will create a PE will depend on the functionality of the server or servers as well as the business activities in the United Kingdom.

UK diverted profits tax

Introduced in the Finance Act 2015, the 'Google tax' was created to counter the use of aggressive tax planning techniques by multinational enterprises to divert profits from the United Kingdom. It is charged at 25 per cent when a foreign company artificially avoids having a UK-taxable PE or when a UK company, or a foreign company with a UK PE, would benefit from a tax advantage (ie, a reduced UK tax liability) through the use of group structures, entities or transactions that lack economic substance.

HMRC will consider various aspects of the structure, including the allocation of profits throughout the supply chain. (See generally the HMRC International Manual.)

Withholding taxes

Withholding taxes may apply at the rate of 20 per cent to sales, services and (in broad terms) income derived from annual payments, patent royalties and certain other payments arising from the exercise of intellectual property rights paid by a UK resident company to a non-UK resident person who is not a corporate taxpayer, subject to reduction under an applicable tax treaty. For example, withholding taxes may apply where, in a CSP group structure, a non-UK, IP rights-owning or licensor group company has put in place intra-group IP rights licensing arrangements and the UK-based group CSP is required to remit payments to the non-UK licensor for the exploitation, licensing or distribution of that IP right. Legislation was enacted in the United Kingdom in 2016 to address the abuse of double taxation treaties in this context.

Offshore receipts in respect of intangible property

In 2019, the UK government introduced an income tax charge on offshore receipts from intangible property (ORIP). From 6 April 2019, non-UK residents in certain (generally low-tax) jurisdictions have been liable to UK income tax on their gross receipts from intangibles to the extent the IP enables, facilitates or promotes UK sales. The aim is to ensure that businesses generating income from UK sales are not able to artificially achieve low effective tax rates by holding their IP offshore. ORIP applies only if UK sales by the non-UK resident (and its connected persons) for a given tax year exceed £10 million, but it applies whether or not the non-UK resident has any presence in the United Kingdom. Several exemptions are available from the charge.

Businesses will need to determine whether their IP enables, facilitates or promotes UK sales, either directly or indirectly, and even through unrelated parties. Taxpayers may find it difficult to trace through often complex supply chains to determine whether their IP is supporting UK sales.

Taxing the digital economy

The UK government introduced a new digital services tax in April 2020. It was introduced as an interim measure until a multilateral solution that is acceptable to the UK is adopted. Discussions are underway between different countries which could see digital services taxes repealed in return for the introduction of 'Pillar One', which would allow allocation of taxing rights for the most profitable and largest companies outside of the jurisdiction where they have an existing tax presence.

The UK government stated that it intends to disapply its digital services tax once an appropriate international solution is in place. In its digital services tax, the UK has focused on 'user participation'. The government views user participation as being a key value driver for digital businesses and the legislation targets digital business models, where value is actually created as a result of the active participation and engagement of UK users of digital platforms. The business models that are impacted by the UK digital services tax include online marketplaces, social media platforms and search engines. To the extent that these models are served by cloud computing services and CSPs, they are likely to be relevant to the cloud computing industry operating in, or that target customers in, the United Kingdom.

The digital services tax applies to revenue earned from 1 April 2020. Businesses are liable to the tax when the group's worldwide revenues from in scope digital activities are more than £500 million and more than £25 million of these revenues are derived from UK users.

If the group's revenues exceed these thresholds, its revenues derived from UK users is taxed at a rate of 2 per cent. The first £25 million of the UK revenues are exempt from the digital services tax. These thresholds mean that only the very largest multinationals are caught, so while CSPs may be involved with in-scope activities, the thresholds may exclude them in practice.

Indirect taxes

25 Outline the indirect taxes imposed in your jurisdiction that apply to the provision from within, or importing of cloud computing services from outside, your jurisdiction.

Both CSPs and cloud customers are advised to seek specific advice on indirect tax questions relating to UK cloud operations and service arrangements.

The rules outlined below applied up to and including 31 December 2020, when the transition period for the United Kingdom's departure from the European Union ended. There is significant uncertainty about whether the new regime will replicate or alter the current rules. We advise readers to be aware of the potential for significant change in this area.

The rules for applying VAT to electronically supplied services differ depending on:

- whether the CSP and its customers are inside or outside the United Kingdom or the European Union;
- whether the cloud services are for business or personal use; and
- if they are supplied as a B2B service, whether they are used and enjoyed within the United Kingdom, within the European Union, or outside of both.

A UK CSP will need to VAT register and will be liable to charge and account for VAT on the supply of cloud services delivered in the United Kingdom. However, supplies within a VAT group are generally disregarded for VAT purposes.

Non-UK suppliers will generally not need to register for VAT in the United Kingdom. For B2B transactions to a UK customer, VAT will generally be chargeable at the standard rate of 20 per cent. The customer will need to apply the reverse charge and may be able to recover the VAT depending on the outbound supplies it makes.

For business-to-consumer transactions, the place of supply will generally be where the supplier belongs. If the supplier is in the United Kingdom, UK VAT will generally be chargeable.

Non-EU CSPs providing cloud services to UK consumers are subject to a special set of rules. The supply is treated as being made at the consumer's place of residence. The CSP will be required to register for VAT.

Until 31 December 2020, HMRC operated a scheme called the 'VAT Mini One Stop Shop' that allowed non-EU suppliers to account for VAT on supplies to the United Kingdom and the European Union under one registration. However, this scheme was withdrawn on 1 January 2021.

RECENT CASES

Notable cases

26 Identify and give details of any notable cases, or commercial, private, administrative or regulatory determinations within the past three years in your jurisdiction that have directly involved cloud computing as a business model.

There have been no recent cases in the last three years involving discussions about cloud computing as a business model specifically, as the provision of IT services via the cloud has become accepted business practice.

However, CSPs may face difficulties using the word 'SKY' in the United Kingdom for cloud services (evidenced by the number of cases in the period 2013-2018 involving the potential confusion arising from the use of the word 'SKY' in connection with cloud services), culminating in the decision of the Court of Appeal in a recent trade mark case.

Sky Limited and others v SkyKick, UK Ltd and another [2021] EWCA Civ 1121 concerned the use of 'Sky'-prefix marks by cloud migration company SkyKick in relation to its cloud technology offering. The court held that use of 'SkyKick' in relation to an email migration service (cloud migration) and a backup service (cloud backup) did infringe Sky Ltd's trademarks for 'SKY' in relation to 'electronic mail services' and 'computer services for accessing and retrieving audio, visual and/or audio-visual content and documents via a computer or computer network' and SkyKick was unsuccessful in its efforts to limit the very wide specification of goods/services for which Sky had registered its marks (to exclude services relating to cloud computing) and demonstrate bad faith on the part of Sky regarding its trade mark registration strategy.

Similar disputes have arisen about the use of the word 'cloud'. For example, in the 2017 case of *Massive Bionics v EUIPO*, the European General Court partially upheld an opposition by Apple to the registration of 'Dricloud' for cloud services by Massive Bionics on the basis that this sign was similar overall to Apple's trade mark 'iCloud' also covering cloud services. Also, in *Clouds Sky GmbH v EUIPO* (Case T-738/19), Cloud Networks Ltd filing a mark for 'Wi-Fi Powered by The Cloud' was the subject of an unsuccessful challenge by Clouds Sky GmbH, which was unable to show, based on the evidence it submitted to the Board of Appeal, that the word 'cloud' was descriptive, and therefore that the Cloud Networks' trade mark, which included the word 'cloud' and an image of a cloud, was therefore invalid for lack of distinctiveness.

An interesting criminal case (while not directly on point) illustrated the near-ubiquity of cloud computing services when a judge amended the conditions of an order which restricted an offender using computers, mobile phones with internet access and remote storage, stating that these restrictions were disproportionate and unenforceable, in part because the order contained restrictions that the offender could not: own, possess or use any computer other than what he could use at a public library; subscribe to or utilise any 'cloud' or similar remote storage media; or own or use any mobile phone capable of accessing the internet. The judge specifically commented on the fact cloud storage was practically built into most operating systems and any device the offender used (including in public libraries) would contravene the prohibition in the order, and therefore quashed these aspects of the order on the grounds they could not be enforced in practice.

The Competition and Markets Authority (CMA) also issued a merger clearance decision in October 2020 as regards the acquisition by Sinch Holding AB of the SAP Digital Interconnect Unit from SAP SE. This explored the market dynamics for cloud services where the parties overlapped in the supply of cloud communications platform as a service (CPaaS). The merger was not referred for further investigation, as the CMA concluded that since the market for the supply of CPaaS in the UK is still emerging, the current position of the parties was likely to be an imperfect guide to future competition. The CMA held that the parties were not better or worse placed to develop CPaaS than other application-to-person SMS retail suppliers and that there would remain sufficient competitors post-merger to compete with the merged entity.

Antitrust and competition authorities globally have increased their enforcement activities in the big tech space and many of the tech companies are facing parallel regulatory investigations across a number of product lines. However, none are facing any such actions in the United Kingdom regarding the provision of cloud services at the time of writing.

UPDATE AND TRENDS

Key developments of the past year

27 What are the main challenges facing cloud computing within, from or to your jurisdiction? Are there any draft laws or legislative initiatives specific to cloud computing that are being developed or are contemplated?

On 17 May 2021, the Department for Digital, Culture, Media and Sport published a policy paper on cybersecurity in supply chains and managed service providers. It is seeking input on how organisations across the market manage supply chain cyber risks and what additional government intervention would enable organisations to do this more effectively, and the suitability of a proposed framework for the security of managed service providers and how this framework could be implemented to ensure adequate baseline security to manage the risks associated with the use of managed service providers. This reflects the increased use of cloud services by UK businesses and concerns about risks to digital supply chains exposed by the SolarWinds hacking. It is likely to lead to the development of enhanced cybersecurity standards and incentivising providers to take increased responsibility for security outcomes.

The paper states that currently under the Network and Information Systems Regulations (as currently scoped) cloud computing services are subject to much less stringent regulatory oversight than other entities under the Regulations. For example, the ex-post supervisory regime ensures that regulatory scrutiny applies to cloud service providers only in the aftermath of an incident. However, most managed service providers are not within the scope of the definition of 'digital service provider' and are therefore not subject to the Network and Information Systems Regulations. The policy paper includes proposals for legislative changes to better address managed service provider resilience.

* *The authors would like to thank BCLP colleagues Kate Brimsted, Jack Dunn, Anne Powell, David von Hagen, Rachel Dale, Sandy Aziz, Farhana Shaikh and Sophie Shaw for their assistance in writing this chapter.*

Marcus Pearl
marcus.pearl@bclplaw.com

Anna Blest
anna.blest@bclplaw.com

Governor's House
5 Laurence Pountney Hill
London
EC4R 0BR
United Kingdom
Tel: +44 20 3400 1000
www.bclplaw.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-634-1