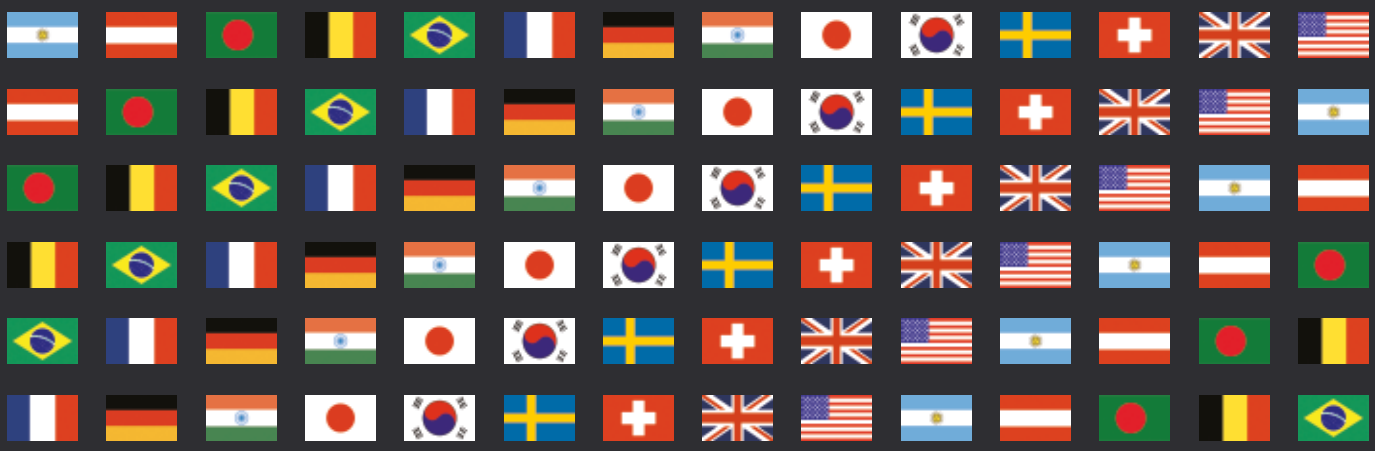
Cloud Computing 2020

Contributing editor
Mark Lewis



LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House
34–35 Farringdon Street
London, EC4A 4HL
United Kingdom

First published 2017
Third edition
ISBN 978-1-83862-164-3

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

Cloud Computing
2020

Contributing editor
Mark Lewis
Bryan Cave Leighton Paisner LLP

Lexology Getting The Deal Through is delighted to publish the third 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. Our coverage this year includes a new chapter on Austria.

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 editor Mark Lewis of Bryan Cave Leighton Paisner LLP, for his continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
October 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2019
For further information please contact editorial@gettingthedealthrough.com

United Kingdom

Mark Lewis*

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 IT and related services markets, the UK is one of the most important global markets for cloud computing. According to Gartner, judged by cloud spending rates and growth, the UK is among the fastest cloud adopters globally, ranking behind the USA (the world leader in cloud adoption since 2015) and Canada: https://www.gartner.com/smarterwithgartner/cloud-adoption-where-does-your-country-rank/. In its 2018 BSA Global Cloud Computing Scorecard (the latest version since first publication in 2012 and claimed 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 at fourth after Germany, Japan and the USA. To account for the difference in the UK's standing in these two reports, it is worth explaining that the BSA Global Cloud Computing 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: https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf. Other market analysts, such as MarketsandMarkets™ (https://www.marketsandmarkets.com/), 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 the more rapid adoption of cloud services in the UK.

Using the US National Institute of Standards and Technology (NIST) definition of cloud computing (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf), 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 (deployment models)), private, public and hybrid clouds are widely adopted. Community clouds are also used, though apparently 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, enabling their customers 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 government of cloud computing. In 2012, the UK government introduced the G-Cloud, 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, for example Amazon Web Services (AWS) (http://searchcloudcomputing.techtarget.com/definition/G-cloud-government-cloud). In February 2017, the UK government reaffirmed the Government Cloud First Policy, under which public sector organisations must consider and evaluate potential public cloud 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: www.gov.uk/guidance/government-cloud-first-policy. For the origins of this important cloud initiative, see the UK government's 2011 paper, Government Cloud Strategy, at: www.gov.uk/government/publications/government-cloud-strategy. 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 (www.outsourcery.co.uk/about-us/news/public-sector-cloud-adoption-soaring/). However, although adoption of cloud services by UK local government still lags behind central government's rate of deployment, the adoption rate at local government level is apparently steadily increasing.

In May 2019, it was reported in the UK technology sector media that the UK government's Cloud First policy is under review and that it is likely to be replaced by an updated approach that reflects the growing demand for hybrid cloud deployment in the public sector: https://www.computerweekly.com/news/252463001/Government-cloud-first-policy-under-review-by-CCS-and-GDS.

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.

Active global providers

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

All are active in the UK, including (as a small sample):

- Accenture;
- Adobe;
- AWS;
- Avaya;
- Cisco;
- Citrix;
- Dell EMC;
- Dropbox;
- Equinix;

- Facebook;
- Google;
- Huawei;
- IBM;
- Interoute;
- Joyent;
- Kaspersky;
- Microsoft;
- NetApp;
- Oracle;
- Rackspace;
- Red Hat;
- SalesForce;
- SAP;
- SAS;
- Skype;
- Sungard;
- Symantec;
- VMware; and
- Workday.

(See www.cloudpro.co.uk/providers.)

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: RedstoneConnect, ElasticHosts, Fasthosts, Flexiant, Memset, and VMhosts;
- managed services: BT, Claranet, Colt, Interoute, iomart, IT Lab, Nasstar, TIG and Webfusion;
- data backup and security: BT, Cloud Direct, iomart, IT Lab, Memset, RedstoneConnect, TIG, UKFast, UK2 and Vodafone;
- hosted desktop: Colt, Nasstar and Vodafone; and
- channel enablement, go-to-market, digitisation and CRM: BCSG and NewVoiceMedia.

(See www.computerweekly.com/tutorial/UK-hosted-desktop-cloud-providers; noting that this study was undertaken in 2010 and that it has not been updated since.) For various cloud services mainly focused on the UK public sector, there is UKCloud: https://ukcloud.com/.

Market size

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

See question 1 for the findings of Gartner and BSA|The Software Alliance.

Research undertaken and provided to the author by MarketsandMarkets suggests that in 2019 the UK's cloud computing market will be worth £20.3 billion, rising to £22.8 billion in 2020 (a 12.3 per cent increase from 2019) and £35.1 billion by 2023 (a 73 per cent rise from 2019): source, private research provided to the author by MarketsandMarkets in September 2019, based on primary interviews, secondary literature and MarketsandMarkets analysis.

According to the MarketsandMarkets report referred to above, in 2020 the size of the UK's cloud computing market by service model will be as follows: SaaS £14.3 billion; PaaS £2.1 billion; and IaaS £6.4 billion.

The same MarketsandMarkets report forecasts that, in 2020, the size of the UK's cloud computing market for the three main deployment models will be as follows: private cloud £5.1 billion; public cloud £10.9 billion; and hybrid cloud £6.8 billion.

Impact studies

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

Authoritative, specific, recent data on the true size and therefore impact of cloud computing in the UK is hard to find. And such reports are not in the author's experience freely available to the general public, online or otherwise. See the three reports referred to under questions 1 and 4. Of the three, the MarketsandMarkets report referred to above 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.

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 (www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy). The stated core aim of the policy is 'to create a world-leading digital economy that works for everyone. It is part of this government's Plan for Britain, strengthening our economy for the long term as we take advantage of the opportunities that leaving the European Union provides.' (Ministerial foreword, page 2.)

There are seven elements to this policy, together with a framework for action:

- connectivity – building world-class digital infrastructure for the UK;
- digital skills and inclusion – giving everyone access to the digital skills they need;
- the digital sectors – making the UK the best place to start and grow a digital business;
- the wider economy – helping every British business become a digital business;
- a safe and secure cyberspace – making the UK the safest place in the world to live and work online;
- digital government – maintaining the UK government as a world leader in serving its citizens online; and
- data – unlocking the power of data in the UK economy and improving confidence in its use. The paper affirmed the UK's commitment to implementing the General Data Protection Regulation (GDPR) by May 2018 (https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr). Accordingly, the Data Protection Act 2018 came into force on 25 May 2018. The Act incorporates the GDPR into law in the UK and supplements its provisions.

In April 2017, the Digital Economy Act 2017 was enacted to implement the government's digital strategy (www.gov.uk/government/collections/digital-economy-bill-2016 and www.legislation.gov.uk/ukpga/2017/30/contents/enacted). 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 (see question 7), that the policy and implementation framework embraces all the cloud service models and deployment models. And, as outlined in question 1, the UK government is a world leader in its deployment of cloud computing through its Government Cloud First Policy.

Incentives

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

Yes. 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 as well as more mature technology companies. They generally cover: tax incentives for the companies themselves as well as 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
Offering tax efficient benefits to investors in return for investment in small and early stage start-up technology businesses in the UK (www.seis.co.uk/about-seis).

The Enterprise Investment Scheme
Also offering tax benefits to investors in technology companies (https://www.gov.uk/guidance/venture-capital-schemes-apply-for-the-enterprise-investment-scheme).

R&D tax credits
Available for both small and medium-sized enterprises (SMEs) and larger companies (at different levels), tax credits for qualifying R&D, which may include subcontractor costs, supporting software and SaaS, and some hardware costs: https://granttree.co.uk/tax-credits/#r&d-tax.

The Patent Box
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 (www.gov.uk/guidance/corporation-tax-the-patent-box).

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 at July 2019, competitions include the opportunity to apply 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, and the chance to obtain loans for 'game-changing' innovations with strong commercial potential that will significantly improve the UK economy (www.gov.uk/guidance/innovation-apply-for-a-funding-award and https://apply-for-innovation-funding.service.gov.uk/competition/search).

Regional growth funds
Grants and loans of up to £1 million are available through regional growth funds (RGF) programmes, namely schemes run by national or local organisations that have been awarded RGF funds to offer grants and loans to eligible businesses. The schemes have invested a total of £2.6 billion in eligible businesses since the launch of the RGF in 2010. Each RGF programme will have specific criteria for applications (https://www.gov.uk/guidance/understanding-the-regional-growth-fund).

The British Business Bank and enterprise capital funds
The British Business Bank (TBBB) invests alongside venture capital funds (partners) under a rolling programme. Funding is aimed at smaller UK growth companies. One of TBBB's partners, Notion Capital, invests in enterprise SaaS and other cloud computing businesses. In July 2015, Notion Capital announced a US$120 million fund that would continue to invest in European business-to-business (B2B) high-growth SaaS companies (british-business-bank.co.uk/british-business-bank.co.uk/british-business-bank-partner-notion-capital-launches-new-fund/; www.notioncapital.com/about/; and https://notion.vc/portfolio/filter/sector/cloud-services/).

LEGISLATION AND REGULATION

Recognition of concept

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

Except as mentioned in question 9, no, not specifically.

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 Regulations 2018 (www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf), which implement the NIS Directive (2016/1148/ EU), specifically govern a 'cloud computing service', meaning 'a digital service that enables access to a scalable and elastic pool of shareable computing resources': regulation 1(2). Cloud service providers (CSPs) who 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 systems. RDSPs are also required to notify within 72 hours 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. 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.

The ICO has issued a detailed and helpful Guide to the NIS Regulations, which as a first step all CSPs operating in the UK should consult: https://ico.org.uk/for-organisations/the-guide-to-nis/. Included in the Guide are pointers to the cloud services to be governed by the Regulations. The Guide states that PaaS and IaaS service models will be covered, but that SaaS will only be regulated to the extent that the service is 'scalable and elastic' and B2B. Readers are also referred to the UK National Cyber Security Centre's guidance at: www.ncsc.gov.uk/guidance/introduction-nis-directive.

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 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 ecosystem 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 referred to under question 12 and data protection law referred to under question 15), the following are likely to apply to cloud computing (or elements of it) in the UK:

- Digital Economy Act 2017 (www.legislation.gov.uk/ukpga/2017/30/contents/enacted – see question 6);
- Investigatory Powers Act 2016 (as amended) (www.legislation.gov.uk/ukpga/ 2016/25/contents/enacted – interception of communications and retention of communications data, etc);
- EU Dual-Use Regulation 2009, Council Regulation (EC) No 428/2009 (and associated legal amendments) (www.gov.uk/guidance/controls-on-dual-use-goods – regulates the export of dual-use technologies and software);
- Export Control Order 2008: www.legislation.gov.uk/uksi/2008/3231/contents/made – controls on the export of military and certain other technologies and software;
- Communications Act 2003 (www.legislation.gov.uk/ukpga/2003/21/contents – overall regulatory structure and powers for communications and media in the UK, including the regulator, Ofcom);
- Export Control Act 2002 (www.legislation.gov.uk/ukpga/2002/28/contents – controls on the export of, among others, strategic technologies);
- Regulation of Investigatory Powers Act 2000 (www.legislation.gov.uk/ukpga/2000/23/introduction – interception of communications and data retention, etc) as amended; and
- Unfair Contract Terms Act 1977 (www.legislation.gov.uk/ukpga/1977 – makes unenforceable certain terms in B2B contracts that do not satisfy the requirements of 'reasonableness').

The above is not an exhaustive list, and readers should also consider other areas covered by UK legislation and regulation, for example regarding intellectual property rights and employment law, some of which are covered below.

Apart from legal and regulatory enactments, particularly in the context of cloud computing, readers should be aware of various international law enforcement measures under treaty 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 (MLA). (See, for example: the Council of Europe Convention on Cybercrime 2004, ETS No. 185 at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461&back=5441; and the UK's (then) proposed bilateral ratification of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at www.gov.uk/government/uploads/system/uploads/attachment_data/file/238612/7613.pdf.)

Although beyond the scope of this section, readers will be aware of the extraterritorial impact of the USA PATRIOT Act on cloud services (www.wired.com/insights/2011/12/us-cloud).

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 – again 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 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' – for an overview, see www.cloudindustryforum.org/content/code-practice-cloud-service-providers). 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 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, though it too is not legislation or public regulation, 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' (www.asa.org.uk/about-asa-and-cap.html). 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 website for five years (www.asa.org.uk/codes-and-rulings/rulings.html.) Though ASA rulings do not have any legal effect, an adverse ruling may have 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 – who do have legally enforceable powers and the ability to impose legal sanctions – for further action, for example UK Trading Standards or Ofcom (the communications regulator) (www.asa.org.uk/codes-and-rulings/sanctions.html). It is worth noting that the ASA has in the past considered several specific cloud computing-related advertisements and has found against advertisers (www.asa.org.uk/rulings/jdi-backup-ltd-a14-260786.html, www.asa.org.uk/rulings/jdi-backup-ltd-a13-226451.html; www.asa.org.uk/rulings/jc-inc-a12-215093.html; www.asa.org.uk/rulings/uk-2-ltd-a13-252423.html).

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. (For the CIF Code and ASA codes, see question 10.)

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 (www.legislation.gov.uk/uksi/2002/2013/contents/made);
- the Consumer Protection from Unfair Trading Regulations 2008 (www.legislation.gov.uk/uksi/2008/1277/contents/made);
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (www.legislation.gov.uk/uksi/2013/3134/contents/made); and
- the Consumer Rights Act 2015 (www.legislation.gov.uk/ukpga/2015/15/contents/enacted).

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.

Other legislation includes:

- the Financial Services and Markets Act 2000 (www.legislation.gov.uk/ukpga/2000/8/contents (FSMA));
- the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (www.legislation.gov.uk/uksi/2001/544/contents/made); and
- the Consumer Credit Act 1974 (as amended) (www.legislation.gov.uk/ukpga/1974/39).

Together these regulate B2C credit terms, including any form of 'financial accommodation', and specify certain contract terms and restrictions (with 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 Competition and Markets Authority (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 found that some CSPs were using contract terms and practices that it was concerned could breach consumer protection law ('An open letter to cloud storage providers on complying with consumer law', May 2016, www.gov.uk/government/uploads/system/uploads/attachment_data/file/526355/open-letter-cloud-storage-providers.pdf.) 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 (www.gov.uk/government/news/cma-secures-better-deal-for-cloud-storage-users).

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 the examination of sector-specific legislation, regulations, guidance and regulatory and statutory codes of conduct. In the UK – and with the exception of the NIS Regulations referred to in question 9 and the following example – at the time of writing this chapter 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.

Only in the UK financial services sector has cloud computing been specifically addressed. Operational resilience, including outsourcing to the cloud, has been identified as a cross-sector priority in the Financial Conduct Authority (FCA),'s annual regulatory business plans for the past several years. The FCA, Bank of England and Prudential Regulation Authority (PRA) issued a joint Discussion Paper (18/4) in July 2018 on operational resilience, which stressed the importance of understanding and mapping important third party providers. Issues identified in the Discussion Paper will be developed into joint policy proposals later in 2019.

In July 2016, the FCA issued its finalised FG 16/5 – 'Guidance for firms outsourcing to the 'cloud' and other third-party IT services' (www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it; www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf (FCA Cloud Guidance)). In July 2018, the FCA Cloud Guidance was modified as mentioned below. While some regulatory objectives are issued by the FCA and the PRA as 'guidance' (as opposed to rules), it would be a foolhardy regulated financial services organisation that disregarded such guidance or diluted it too far in application.

Before outlining the FCA Cloud Guidance, it must be put in its sectoral regulatory context. When financial services organisations (firms) regulated under FSMA (see question 12) 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 conduct of business of all financial services organisations within its statutory jurisdiction, including those prudentially supervised by the PRA. Some outsource providers (who, incidentally, are also CSPs) are themselves authorised and regulated by the FCA.

The PRA and FCA rules are complex and their application to 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. The main rules and guidance governing outsourcing by regulated firms are contained in the FCA Handbook and PRA Rulebook. There is also more general FCA guidance on outsourcing to meet FSMA compliance. These are the main sources of prudential and operational provisions regulating outsourcing by financial services firms and regulated outsource providers in the UK. 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 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563889385175&uri=CELEX:02009L0138-20190113 and https://www.bankofengland.co.uk/prudential-regulation/key-initiatives/solvency-ii).

The detailed rules governing outsourcing under the PRA Rulebook, FCA Handbook, Solvency II Directive and Solvency 2 Regulations 2015 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 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 (for a fuller statement, see the FCA Handbook, Systems and Controls (SYSC), chapters, 3, 4, 8, 13 and 14: www.handbook.fca.org.uk/handbook/SYSC/).

The Markets in Financial Instruments Directive (MiFID) II (2014/65/EU), which repealed and recast the MiFID Directive (2004/39/EC) and (largely) entered into force on 3 January 2018, together with the Delegated Regulation (2017/565/EU) (commonly referred to as the MiFID Organisation Regulation or the MiFID Org Regulation), imposes on regulated firms a wide range of conduct of business and organisational requirements. These include requirements relating to outsourcing, as well as more general record keeping and business continuity issues. The FCA handbook was updated to reflect these requirements.

The European Banking Authority (EBA) published finalised Guidelines on Outsourcing Arrangements (EBA Guidelines) on 25 February 2019: https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements. The EBA Guidelines apply from 30 September 2019, and firms must amend existing outsourcing arrangements to comply with the EBA Guidelines by 31 December 2021. They apply to credit institutions and investment firms, as well as to authorised payment institutions and e-money institutions.

The EBA Guidelines are divided into five sections, or Titles: (I) Proportionality: group application and institutional protection schemes (setting out a principle of proportionality in application of the EBA Guidelines, and requiring transparency within groups); (II) Assessment of outsourcing arrangements (defining 'outsourcing' and 'critical or important' functions); (III) Governance framework; (IV) Outsourcing process (setting out aspects to be included in an outsourcing agreement at a minimum for a critical or important function); and (V) 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. EBA Guidelines on internal governance published in March 2018 should also be taken into account.

The EBA Guidelines replace the Committee of European Banking Supervisors Guidelines on Outsourcing published in 2006, and incorporate the EBA Recommendations on Outsourcing to Cloud Service Providers (which were applicable from 1 July 2018). The FCA Cloud Guidance was updated in July 2018, to confirm that the FCA Cloud Guidance does not apply to a bank, building society, designated investment firm or IFPRU investment firm to whom the EBA Recommendations are addressed: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf. The FCA has confirmed that it will keep its Cloud Guidance under review to assess what, if any, changes are required, including as a result of Brexit. In the interests of space, this section now focuses on the FCA Cloud Guidance.

The FCA Cloud Guidance is addressed to such firms (see previous paragraph) 'when outsourcing to the "cloud" and other third party IT services'. As is evident from the FCA Cloud Guidance, for the FCA, not only is cloud computing 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 private, public or hybrid cloud deployment (paragraph 1.4 FCA Cloud Guidance). And it says that '[from] a regulatory perspective, the exact form of the service used does not, in itself, alter the regulatory obligations placed on firms'. So, where a third party (including a CSP) delivers services on behalf of a regulated firm, this is considered outsourcing. Firms therefore need to consider the relevant regulatory obligations and how they comply with them.' (Paragraph 3.3 FCA Cloud Guidance.)

The stated aim of the FCA Cloud Guidance is to facilitate 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).

Apart from the regulated firms themselves, the FCA Cloud Guidance is stated to be of interest to third-party IT providers, trade associations and consumer groups, professional advisers and the auditors of regulated firms.

In outline and focusing below on the most important aspects of the FCA Cloud Guidance for cloud computing, the regulated firm in scope of the FCA Cloud Guidance must have regard to the following.

Criticality or materiality of the cloud service

Whether the function being processed under the cloud service is 'critical or important' or 'material' and (for authorised payment institutions and authorised electronic money institutions) if it relates to 'important operational functions'. Each of these terms is defined in the FCA Handbook and the Electronic Money Regulations 2011 (www.legislation.gov.uk/uksi/2011/99/contents/made and Payment Services Regulations 2009: www.legislation.gov.uk/uksi/2009/209/contents/made; paragraph 3.6 FCA Cloud Guidance); and see also the EBA Guidelines section 4, and paragraph 20 of the accompanying EBA Final Report. Overall, if the above kinds of functions are 'outsourced' to the cloud, firms in scope of the FCA Cloud Guidance will have more stringent duties with regard to management of operational risk in the transaction, as will CSPs in enabling firms to comply with their obligations. In addition, firms must notify the FCA when entering into or significantly changing material or critical cloud services arrangements (paragraph 3.7 FCA Cloud Guidance).

In some cases, dual-regulated firms subject to the PRA's preferred resolution strategy will also have to consider resolution arrangements when entering into cloud services projects. These arrangements are designed to ensure continuity in distressed economic circumstances or insolvency to ensure that 'critical economic functions' are maintained (paragraph 3.8 FCA Cloud Guidance and https://www.bankofengland.co.uk/financial-stability/resolution).

Legal and regulatory considerations

These include having a business case or rationale for the decision to outsource to the cloud and the use of one or more CSPs for the delivery of critical or important operational functions, or a material outsourcing; due diligence risk assessment of the proposed project; relative risks of each type of cloud service or deployment model (eg, private versus public cloud); knowing where the CSP service and other relevant locations are situated; and the need to identify all service providers in the cloud supply chain – to ensure that the regulatory requirements are met throughout the supply chain.

Risk management

Including: conducting and documenting a risk assessment of the proposed cloud project; monitoring concentration risk, to avoid too great a dependency on any one CSP; and understanding what action to take if the CSP failed.

International standards

Including: as part of due diligence, assessing the CSP's adherence to accepted international IT and service standards; and applying greater standards of assurance when the functions concerned are critical or important or a material outsourcing.

CSP oversight

Including: clarity about the allocation of responsibilities between the firm and the CSP; the firm having an internal function responsible for the strategic and day-to-day management of the CSP; and ensuring that the firm's staff have sufficient skills and resources to oversee and test the cloud services and properly manage an exit or migration from the existing CSP. In other words, this would mean firms having and retaining specific cloud service management expertise.

Data security

Including: conducting a specific risk assessment; agreeing data residency terms with the CSP, setting out contractually the locations in which the firm's data can be stored, processed and managed; considering how the firm's data will be segregated (for public cloud); assessing the sensitivity of data and how the data will be transmitted, stored and encrypted, where necessary – noting that encryption keys or other forms of authentication must be accessible to the FCA or PRA.

Data protection

Including: continuing compliance with data protection laws. Firms are, of course, required separately to comply with UK data protection law

(now the GDPR, as supplemented by the Data Protection Act 2018). In that sense, though the data protection laws are separate, the FCA Cloud Guidance forms part of the firm's compliance with its duties as a regulated firm. Firms should consider the UK Information Commissioner's guidance concerning the transmission of personal data outside the European Economic Area (EEA).

Effective access to data

'Data' is used here in its widest meaning. Firms should ensure that the cloud computing arrangement has addressed the following: access for the firm, their auditors, the regulators and other competent authorities to the firm's data; contractual ability for the regulators to contact the CSP directly where the firm cannot for any reason disclose the data; ensuring that the data is not stored in jurisdictions that may prevent or inhibit effective access for UK regulators; geopolitical stability as it concerns the data; whether the CSP's jurisdiction provides for data protection; the law enforcement provisions of the relevant jurisdiction or jurisdictions where data is to be processed, for example, whether and how easily the authorities in the CSP's jurisdiction may intervene in accessing the firm's data.

Access to business premises

'Premises' here include head offices and operations centres, but not necessarily data centres. The guidance includes: knowing which CSP or supply chain premises are relevant for the cloud services and effective oversight of them (the FCA recognising that CSPs may have legitimate reasons for limiting access to some sites, eg, data centres); providing for the unrestricted contractual and legal ability for the firm or its auditors to request an onsite visit to the business premises – on reasonable prior notice, except in the case of an emergency or crisis; enabling visits by the financial services regulators or other competent authorities as they deem necessary and required by law or regulation, without any conditions being imposed; having the CSP commit contractually to cooperating with all reasonable requests of the regulators during such visits; affording the regulators the right to observe the provision of the cloud services to the firm or any of its affiliates (although the regulators may commit to minimising disruption to the CSP's operations).

Relationship between service providers

Including: considering how the cloud supply chain is constructed and operates; enabling the firm to review subcontracting and other supply chain arrangements to ensure that they facilitate the firm's compliance with its regulatory requirements, including security, effective access to data and business sites; understanding the roles of CSPs within the supply chain; knowing how a CSP's services will interface with the firm's own systems or other necessary third-party systems (eg, agency banking arrangements for payments).

Change management

Including: ensuring that contractual and operational provision is made for changes to the cloud services; and establishing how changes will be tested.

Continuity and business planning

Including: providing contractually and operationally for appropriate arrangements for the continuity of functions and the ability of the firm to meet its regulatory obligations in the event of an 'unforeseen interruption' of the cloud services; having a plan documenting the continuity, business interruption and recovery arrangements; regular testing of the business continuity plan; and putting in place contractual and operational measures to ensure regulatory access to data in an insolvency or other disruption of the cloud services.

Resolution

This guidance will only apply to certain firms (see 'Criticality or materiality of the cloud service' above). In this context, the main aspect of the resolution and recovery arrangements and the Bank of England's 'stabilisation' powers that will concern firms, CSPs and providers within the cloud supply chain is this: neither financial distress or insolvency leading to resolution, nor the change of ownership or control of the firm following that event, will enable the CSP or a cloud supply chain provider to terminate the contract or the provision of cloud services. Moreover, the CSP and its supply chain may have to provide the cloud services to the resolution successor entity or firm for a transitional period. The CSP (and by implication providers in its supply chain) must agree not to delete, revoke or change the firm's data in the case of resolution.

Exit planning

Including: firms having contractually documented exit plans and termination assistance arrangements to ensure continuity, and these plans being 'fully tested'; firms understanding how they would migrate the cloud services to an alternative CSP and maintain business continuity; contractually requiring the CSP (and by implication its supply chain) to cooperate fully with the firm and the incoming CSP to ensure a smooth transition; the firm understanding how it could and would remove its data from the CSP's systems on exit.

The aim of the FCA Cloud Guidance is to help overcome the barriers created by the perceived regulatory uncertainty in the adoption of cloud computing by UK financial services firms. As the FCA says: 'We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.' (Paragraph 1.6 FCA Cloud Guidance.)

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. My own experience and that of my colleagues shows that, 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. In February 2017, the British Bankers' Association (now UK Finance), identified seven barriers to cloud adoption:

- the regulatory approach to 'important' and 'critical' functions;
- supervision and oversight;
- the risk framework;
- access to CSP sites and services by regulators;
- data residency;
- termination; and
- data breaches and monitoring.

Most of these concerns will be identifiable from the FCA Cloud Guidance summarised above and look likely to remain of concern to the financial services sector in the immediate future.

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 (www.legislation.gov.uk/ukpga/1986/45/contents) and the Insolvency (England and

Wales) Rules 2016 (www.legislation.gov.uk/uksi/2016/1024/contents/made) (both as amended). For an overall guide to the UK insolvency regime, see www.pwc.co.uk/assets/pdf/insolvency-in-brief.pdf.

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. And 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 (http://diginomica.com/2015/01/06/cios-worst-nightmare-cloud-provider-goes-bankrupt/). 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 (www.legislation.gov.uk/uksi/2015/989/article/2/made). The amendments introduced by the 2015 Order ensure that, like utility services, 'communication services' and other IT supplies will now be 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' (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.

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 comprises the GDPR and the Data Protection Act 2018 (DPA). The DPA is the UK's implementation of the GDPR; although the DPA also supplements the GDPR in certain areas. It is the successor to the previous Data Protection Act 1998. The 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 DPA, the ICO states that it 'still considers the information useful'. At the time of writing, the ICO has confirmed 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 GDPR and the DPA.

General knowledge of the principles of the 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 GDPR. The following focuses on certain elements of the 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 GDPR.

Territorial scope

The GDPR applies to the processing of personal data within the context of the activities of an establishment of a controller or processor in the EU, regardless of whether such processing takes place in the EU or not. Clearly, the GDPR applies to the processing of personal data of a controller or processor in the EU; in addition, draft guidelines from the European Data Protection Board at the time of writing 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 GDPR will also apply to the processing of personal data of data subjects in the EU by data controllers and processors with no EU establishment where the processing relates to offering goods and services (free or for payment) to EU data subjects, or to monitoring the behaviour taking place in the EU of such data subjects (article 3(2)). The GDPR applies, therefore, to CSPs (assuming them to be either processors or controllers) without sites in the EU, if they meet either or both of the above tests. Certain controllers or processors (including CSPs) will have to appoint a local EU 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, determining the purposes and means of the processing of personal data (article 4(7)). It will be in the interests of CSPs to ensure that this characterisation continues under the GDPR, as ultimately the controller will be bound by more stringent duties than the processor. The challenge in B2C cloud computing, especially for social media and network services, is how CSPs ensure that their standard public cloud contract terms maintain consumer customers as controllers – if indeed the legislation applies to those consumer contracts at all.

The controller, or cloud customer, will be primarily liable for lawful processing, including 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, for example regulated financial services firms deciding to engage CSPs for their operations, this aspect of the decision will almost certainly have to be documented (see question 13).

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 GDPR obligations (for the current European Union Agency for Network and Information Security (ENISA) framework see www.enisa.europa.eu/news/enisa-news/enisa-cloud-certification-schemes-metaframework/). We should expect to see the development by CSP industry organisations of cloud-specific codes of conduct and certification mechanisms, for example, the CIF Code referred to under question

10; although such codes and certification mechanisms will have to be approved.

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. And 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 (see below); 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 European Commission or the Information Commissioner's Office to date. 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, the 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 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 (see above), additional requirements imposed on processors will 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 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; 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 GDPR controllers and (as mentioned above) processors will be directly accountable and liable for non-compliance, both to data subjects and regulators. The allocation of responsibility and liability for infringements as between cloud customers and CSPs has, therefore, assumed even greater importance in B2B and B2C-related cloud contracts – particularly because of the extent and scale of the 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)).

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 €10 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 €20 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 GDPR and the DPA, 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 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 GDPR framework for such transfers is similar to that under the previous Data Protection Act 1998 and Data Protection Directive, with some useful new 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 (see sanctions and remedies above). Both controllers and processors will be liable to non-compliance proceedings.

Uncertainty looms over the adequacy of the SCCs (also known as model clauses) approved by the European Commission as a means of ensuring adequate protection of personal data when transferred to recipients in third countries. The *Schrems II* litigation (*Facebook Ireland*

& Schrems (Case C-311/18)) (*Schrems II)*, the opening arguments of which were heard in July 2019, concerns whether these clauses provide a sufficient degree of protection for personal data transferred to the US. The SCCs are the most widely used international transfer mechanisms for personal data, meaning that a ruling by the Court of Justice of the European Union (CJEU) invalidating the clauses would have a wide-ranging impact on businesses. The CJEU's judgment is expected to be handed down in early 2020.

Privacy Shield

Adopted by the European Commission in July 2016 (http://europa.eu/rapid/press-release_IP-16-2461_en.htm), this applies to EU–US data transfers and is 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 (https://azure.microsoft.com/en-gb/blog/microsoft-cloud-is-first-csp-behind-the-privacy-shield/). At the time of writing, the Privacy Shield is also under threat, as the European Parliament has issued a resolution requesting that the European Commission suspend the Privacy Shield until such time as the USA can demonstrate full compliance with its terms and this mechanism is also susceptible as a result of the *Schrems II* litigation referred to above.

Access to EU personal data by third country governments

In the light of the Snowden disclosures and the litigation that followed them (eg, *Microsoft v United States*, No. 14-2985 (2d Cir. 2016) http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html), it is worth noting that article 48 of the GDPR contains specific safeguards against third country governments' access to 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, for example a mutual assistance treaty between that third country and the EU or a member state. (See also question 10 on MLAs; and the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461&back=5441.)

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)?

It follows from the answer to question 1 that, in the UK, contracts cover the full range of cloud service and deployment models and reflect the UK's large and sophisticated cloud business ecosystem, including CSP 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. In my 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.

The answers to questions 17 to 22 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. 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), noting that, inevitably there will have been changes to CSA practice and terms since. I also wish to acknowledge the excellent reports and other deliverables produced by the (now decommissioned) SLALOM Project teams, which I used to sense-check my own review of the CSAs referred to above. SLALOM documentation is recommended reading for this area and may be downloaded from the links at: https://cordis.europa.eu/news/rcn/134076_en.html, 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, I 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.

The European Commission actively promotes the development and use of fair standard cloud computing contracts and there will be further developments under this initiative (see https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-service-level-agreements).

Finally, the role of international standards will be ever more important as applied to cloud computing services, service level agreements (SLAs) and CSAs (see for cloud computing and distributed platforms ISO/IEC JTC1 SC38, https://www.iso.org/committee/601355.html).

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 SCCs, the choice of governing law and jurisdiction may be those of the customer's location. Courts (rather than arbitral tribunals) competent in the CSP's jurisdiction are most commonly chosen. US CSPs usually require all customers to commit to compliance with applicable US export controls, sanctions and related laws and regulations.

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 on- 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 (see question 22).

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 – see below), 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. 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 (see below) will not accrue.

Acceptable use policy

The CSAs of all the major CSPs contain an AUP: it has become one of the defining features of CSAs in the UK as 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;
- 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.

As stated above and under question 22, breach of the AUP may entitle the CSP to suspend or terminate the CSA – in some cases, the breach of 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 it has been breached by 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 UK as 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 even without the obligation to notify customers beforehand. Typically, when exercised, variation does not entitle the customer to terminate the CSA.

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 GDPR, all the major CSPs operating within, or providing services to, the EEA introduced detailed data protection and processing terms for incorporation into their CSAs, in some cases in separate addenda or supplements.

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 EEA, 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 at the time of writing, there have been no reported legal challenges emanating from the UK 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 – usually during the 12 months preceding the event giving rise to liability. Liability caps of this kind are sometimes tiered by reference to different services, for example the greater of a specified monetary amount or the total charges paid, depending on the service.

Some CSAs exclude from this limitation the CSP's liability for third-party IPR 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 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
- 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.

Some CSAs disclaim liability for unauthorised access to, and for 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.

Also, typical of many CSAs is that customers will not be entitled to claim for service unavailability for scheduled or unscheduled downtime or other service interruptions.

Indemnities

It is common for the customer to have to indemnify the CSP against the customer's and any end user's:

- 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, gives rise to claims, costs, losses, and so on.

Where there are detailed data processing provisions, including data transfer agreements (see question 19), some CSAs will provide for customer indemnification of the CSP against breach of data protection law caused by the customer or an end user.

For the CSPs' obligations to indemnify or (quite commonly) to defend the customer against third-party IPR infringement claims or final judgments, see question 21.

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 are referred to the SLALOM Project's documentation available from the links at: https://cordis.europa.eu/news/rcn/134076_en.html, using 'slalom' as a search term.

The application of specified service credits is usually expressed to be the sole and exclusive remedy for service-level breaches. 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.

Commonly, CSAs do not provide specific SLA breach reporting mechanisms, which 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 the service level breaches, as well as providing details of them for verification by the CSP, who may retain the option of rejecting the customer's claim.

Some CSAs entitle the CSP unilaterally to vary the SLAs and service credits.

It is usual for CSAs to exclude the operation of the SLA, where for example:

- there is a force majeure event;
- the customer or an end user is in breach of the AUP or other terms of the CSA;
- the services have been lawfully suspended;
- the service outage is attributable to technology not provided by the CSP; and
- the CSP's systems are down for maintenance.

See also question 20 under 'Warranties'.

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 2.0 produced by the US Cloud Standards Customer Council, www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf, which may at the time of publication have been updated and available online).

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?

Typical terms are as follows.

- 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).
- The customer retains IPR in the contents uploaded or created by it in using the cloud service. The CSP may use the contents to provide the cloud service or to comply with regulatory or governmental directions or orders.
- 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 ownership in such suggestions to the CSP.
- The CSP reserves rights in all IPR relating to its cloud services, including IPR in the applications and infrastructure used in providing the services.
- If the cloud services are found, or understood by the CSP, to infringe any third-party IPR, 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 cloud services concerned. 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. 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.

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 (unremedied) 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;
- where the cloud service is dependent on third-party IPR (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);
- contravention of export and sanctions controls laws and regulations; and
- one or more (other) breaches of the AUP or any other term of the CSA by the customer or an end user.

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, and in some cases that the customer will be entitled to retrieve its data (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 (www.legislation.gov.uk/uksi/2006/246/contents/made), as amended by (among others) the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 (www.legislation.gov.uk/uksi/2014/16/regulation/1/made#regulation-1-2) (together, TUPE). TUPE implements in the UK the EU Acquired Rights Directive 2001/23/EC (ARD).

The application of the ARD 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 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', for example protection against dismissal and protection against changes to the transferring staff's terms and conditions of employment. There are also prescribed consultation processes before any transfer (see generally www.acas.org.uk/index.aspx?articleid=1655). Accordingly, if TUPE applies to a cloud computing arrangement (in which one of the key drivers is cost-reduction) the financial implications for both the cloud customer and more particularly the CSP 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 where an in-house IT service ceases to be provided by the customer itself and is then provided by the CSP – or is migrated to another CSP after the initial cloud migration, or 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 be 'essentially dedicated' to the customer; although they may still do work for others (TUPE Regulation 3(3); and see generally www.gov.uk/transfers-takeovers). More significantly for cloud computing arrangements, the activities to be carried out by the CSP must be 'fundamentally the same' as those undertaken previously by the customer's staff (TUPE Regulation 3(2A) www.legislation.gov.uk/uksi/2014/16/regulation/1/made#regulation-1-2).

So, the threshold question 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 migration from 'traditional' IT activities to the cloud (see *Department for Education v Huke and another* UKEAT/0080/12, https://www.bailii.org/uk/cases/UKEAT/2012/0080_12_1710.html; *OCS Group UK Ltd v Jones and another* https://www.bailii.org/uk/cases/UKEAT/2009/0038_09_0408.html).

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 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.

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 www.gov.uk/transfers-takeovers).

And 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 UK or that the cloud services will be provided from an offshore location. If there is an assigned workforce based in Great Britain, TUPE can apply to such arrangements, even if the service is provided from offshore.

In outsourcing transactions, because the application of TUPE is so well settled in the UK, it has become customary for the customer and outsource provider to provide specifically and in some detail in the outsourcing contract for the legal, regulatory and financial implications of TUPE – 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 EU are unaware of the ARD and TUPE.

For the reasons given above, 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.

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 in order 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, an information service or a communications service). Consideration will also need to be given to the location of the 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. (For an invaluable guide see Ernst & Young's Worldwide Digital Tax Guide, www.ey.com/gl/en/services/tax/ey-digital-tax-guide.)

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. Readers – both CSPs and cloud customers – should seek specific advice on direct tax questions relating to UK cloud operations and service arrangements. And for tax and other fiscal incentives available for cloud computing businesses in the UK, see questions 6 and 7.

Corporation tax and permanent establishment (PE)

A company resident in the UK 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 UK through a PE in the UK. In determining whether a PE exists, the UK broadly adopts the OECD definition of PE. If a non-UK resident CSP has a fixed place of business in the UK 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 UK and may be liable to UK corporation tax (currently 19 per cent but reducing to 17 per cent in April 2020). Will the presence of cloud servers in the UK be decisive in the determination of a PE? The HM Revenue & Customs (HMRC) 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 UK.

UK diverted profits tax

Introduced in the Finance Act 2015 to counter the use of aggressive tax planning techniques by multinational enterprises to divert profits from the UK, this tax is also known as the 'Google tax'. 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 www.gov.uk/government/publications/diverted-profits-tax-guidance.) Certain amendments were introduced in the Finance Act 2019, which took effect from 29 October 2018 (see https://www.gov.uk/government/publications/diverted-profits-tax-changes/diverted-profits-tax-amendments) .

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, IPR-owning or licensor group company has put in place intra-group IPR 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 IPR. New legislation was enacted in the UK in 2016 to address the abuse of double taxation treaties in this context. (See, generally, http://taxsummaries.pwc.com/ID/United-Kingdom-Corporate-Withholding-taxes.)

Offshore Receipts in respect of Intangible Property

Following a consultation, the UK government has introduced a new income tax charge on offshore receipts from intangible property (ORIP). From 6 April 2019, non-UK residents in certain (generally low-tax) jurisdictions will be 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 (see: https://www.gov.uk/government/publications/offshore-receipts-from-intangible-property/income-tax-offshore-receipts-in-respect-of-intangible-property). ORIP applies only if UK sales by the non-UK resident (and its connected persons) for a given tax year exceed £10m, but it applies whether or not the non-UK resident has any presence in the UK. There are several exemptions that are currently available and the government has proposed additional exemptions in draft regulations released recently.

It is expected that the final regulations will be made available in Autumn 2019 and that parts of the regulations will have retrospective effect (see https://www.gov.uk/government/consultations/draft-regulations-offshore-receipts-in-respect-of-intangible-property). 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 has announced that it will introduce a new Digital Services Tax in April 2020. This will be introduced as an interim measure, until a multilateral solution that is acceptable to the UK is adopted. The UK government has stated that it intends to disapply the tax once an appropriate international solution is in place. The UK has focused on 'user participation'. The government views user participation as being a key value driver for digital businesses and the legislation will target 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 may be impacted by these proposals include online networks, 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 targeting customers in, the UK.

The digital services tax legislation will be introduced in the Finance Bill 2019-20 and will apply to revenue earned from 1 April 2020. Businesses will become 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 will be taxed at a rate of 2 per cent. The first £25 million of the UK revenues would be exempt from the digital services tax (see https://www.gov.uk/government/publications/introduction-of-the-new-digital-services-tax/introduction-of-the-new-digital-services-tax). These thresholds mean that only the very largest multinationals will be 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.

Again, readers – 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 for applying value added tax (VAT) to electronically supplied services differ depending on whether the CSP and its customers are inside or outside the UK or the EU; whether the cloud services are for business or personal use; and if they are B2B supplies, whether they are 'used and enjoyed' within the UK, elsewhere in the EU or outside it.

A UK CSP will be expected to register and be liable to charge and account for VAT on the supply of cloud services delivered in the UK. However, specific consideration should be given to CSP intra-group arrangements, particularly the structure of, and transactions under, those arrangements. Non-UK principals are not expected to be VAT-registered. For B2B cloud transactions supplied in the UK by a UK CSP VAT at the standard rate of 20 per cent will generally be payable in respect of cloud services. Cloud customers will be expected to account themselves for VAT on payments for services provided by non-UK based CSPs – the cloud customer should act as if it is both the supplier and the customer: it charges itself the VAT and then, assuming that the service relates to VAT taxable supplies that it makes, it can claim the VAT back (so rendering the transaction VAT-neutral). In terms of the CSP, the service is disregarded, and it does not need to account for any VAT. This is called the 'reverse charge', but is also known as a 'tax shift'.

For B2C cloud transactions VAT at the standard rate of 20 per cent will generally be payable. A UK CSP will usually be registered and liable to charge and account for VAT on the supply of cloud services in the UK.

Non-UK CSPs providing cloud services to UK consumers should particularly note that the VAT rules for digital services (eg, webhosting services, internet-streaming services, database storage, supplies of software and software update services, and other electronically supplied services) do not follow the standard place of supply rules. The services are treated as supplied in the 'place of residence of the consumer' (and not the place of residence of the supplier). VAT is, therefore, payable, on, and CSPs are VAT-accountable for, supplies of digital services to UK consumers, regardless of whether the CSPs are established in or outside the EU (www.gov.uk/government/publications/vat-supplying-digital-services-to-private-consumers/vat-businesses-supplying-digital-services-to-private-consumers). Accordingly, a CSP established and operating outside the EU that sells digital services to UK consumers (and consumers in other EU member states) will be required either to register for VAT in each EU member state where it has customers and comply with all local VAT rules, or to register for the EU's VAT Mini One Stop Shop (MOSS) scheme in a single EU member state (which should rationalise the VAT accounting requirements).

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.

Pippa Middleton and James Matthews v Person or persons unknown [2016] EWHC 2354 (QB)

The iCloud account of the sister of the Duchess of Cambridge had been hacked, apparently resulting in the theft of some 3,000 images. Ms Middleton and her then fiancé, Mr Matthews, had successfully applied for an interim privacy injunction against persons unknown to prevent the use, publication or disclosure of the stolen images. In this case, they successfully applied for a continuation of the injunction and the extension of its scope to cover material and information from the iCloud account other than images, because Ms Middleton had good reason to believe that all the information in her iCloud account had been hacked, not just her photographs. As reliance on iCloud and similar B2C storage services grows even more widely, such cases are likely to become more frequent, especially where prominent personalities are involved.

Skyscape Cloud Services Ltd v Sky Plc [2016] EWHC 1340 (IPEC)

Skyscape supplied cloud services to UK public sector organisations under the G-Cloud scheme (see question 1). Sky Plc is a well-known UK provider of broadcast and communications services (including an email service) under the trademark 'SKY'. Sky Plc claimed trademark infringement against Skyscape, the CSP, which sought a declaration of non-infringement (DNI) for its marks 'SKYSCAPE' and 'SKYSCAPE CLOUD SERVICES' as applied to its cloud services. The court found that there was a likelihood that a significant part of the relevant public and therefore the average consumer, seeing the sign SKYSCAPE used for an email service, would confuse it with yet another service offered by Sky Plc. The DNI was refused. This case is mentioned because of the apparent popularity of the word 'sky' in the branding of cloud services and the position of Sky Plc in the UK market, together with its registered SKY trademarks. In the result, Skyscape was rebranded as UKCloud (see question 3, and for the background: www.theregister.co.uk/2016/07/28/skyscape_now_uk_cloud/). Unless CSPs are willing to forgo the use of 'sky' in branding and marketing their cloud services in the UK, cases of this kind will proliferate (see *Sky Plc and others v SkyKick UK Ltd and another* [2018] EWHC 155 (Ch) http://www.bailii.org/ew/cases/EWHC/Ch/2018/155.html; and also *British Sky Broadcasting Group plc and others v Microsoft Corporation and another* [2013] EWHC 1826 (Ch) below). Similar disputes have arisen about the use of the word 'cloud'. For example, in *Massive Bionics v EUIPO*, www.bailii.org/eu/cases/EUECJ/2017/T22316.html, the EU 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 own trademark 'iCloud' also covering cloud services.

Majekodunmi v City Facilities Management UK Ltd and others [2015] UKEAT 0157_15_2509

In this case, the UK Employment Appeal Tribunal (EAT) had to consider whether the claimant had validly served his notice of appeal when the attachments containing his notice could only be accessed by a link to Dropbox, the cloud-based file-hosting service. The EAT rejected the claimant's case, finding that sending a link to where a required document is located online is not 'serving' or 'attaching' that document. Although zip files are a valid form of service, in this case the EAT needed the internet to access the zip file location in the cloud. The file had,

therefore, not 'hit' the EAT's server as a standard attachment to an email would. The EAT then had to decide whether the documents were effectively 'attached' to the email purporting to serve the required notice. It held that they were not, because all that had been provided was a link to another location where the documents could be found – the documents themselves had not actually been attached. This is a significant decision for users of cloud-based file-hosting services such as Dropbox. The case also contains an interesting legal consideration of the cloud storage and transmission technologies used. It will be worth watching the development of court and tribunal rules in this regard.

British Sky Broadcasting Group plc and others v Microsoft Corporation and another [2013] EWHC 1826 (Ch)

The court ruled that Microsoft's 'SkyDrive' mark for cloud storage services infringed British Sky Broadcasting's 'SKY' UK and (EU) Community trademarks. The court's decision was influenced by the fact that consumers were unable to discern any Microsoft connection to SkyDrive as a preloaded app on any device. This finding was supported by evidence that 17 British Sky Broadcasting (Sky) customers had contacted Sky's helpline, because they assumed (in actual confusion) that SkyDrive was a Sky-provided service.

Microsoft contested the validity of Sky's UK SKY trademarks in their application to 'goods and services pertaining to cloud storage'. It alleged that:

> *'sky' is a convenient and common word used by traders to describe or allude to a cloud storage system (be that system a good or a service) such that (a) it is incapable of distinguishing a cloud storage system of one undertaking from that of another, and (b) it should be kept free for use by all traders offering such systems.*

Microsoft also claimed that the word 'sky' would be 'recognized by the average consumer as descriptive of a characteristic of a cloud storage system, namely by indicating that the system is for the storage of data remotely, being notionally in 'the cloud' or 'the sky''. Microsoft's challenge of invalidity was rejected.

Aside from the linguistic and symbolic connections between 'sky' and 'the cloud', the case is also interesting because of the judge's technological comparison between broadband services and certain cloud services. He said:

> *It seems to me that the evidence reveals that there is a close connection between file storage, management and sharing software and the provision of broadband services, including the provision of email services . . . Not all data storage providers are broadband providers but it seems to me that the evidence reveals that a significant number of broadband providers also provide data storage.*

In 2014, Microsoft rebranded 'SkyDrive' as 'OneDrive' (www.techrepublic.com/article/microsoft-renames-skydrive-to-more-confusing-onedrive-amid-legal-complaint/).

BRYAN CAVE LEIGHTON PAISNER BCLP

Mark Lewis
mark.lewis@bclplaw.com

Adelaide House
London Bridge
London EC4R 9HA
United Kingdom
Tel: +44 203 400 1000
Fax: +44 203 400 1111
www.bclplaw.com

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?

None.

* *The author would like to thank BCLP colleagues Faiza Bishi, Kate Brimsted, Sarah Buxton, Gillian Dennis, Daren Kemp, Sophie Taylor, Adam Turner and Ash von Schwan for their assistance in writing this chapter.*

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
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
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
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
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
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 978-1-83862-164-3