KEMP IT LAW

IT Law at the Apex

CLOUD COMPUTING

White Paper

Legal Aspects of Cloud Computing: Cloud Contracting

Richard Kemp

June 2019

LEGAL ASPECTS OF CLOUD COMPUTING: CLOUD CONTRACTING

TABLE OF CONTENTS

FIGURES AND TABLES

LEGAL ASPECTS OF CLOUD COMPUTING: CLOUD CONTRACTING

A. INTRODUCTION

1. **Introduction**. Over the last few years, IT lawyers have seen a significant increase in the number and range of cloud contracts coming across their desks. This trend is set to continue in the months and years ahead as cloud computing comes to be the predominant mechanism for organisations to receive, consume, develop and deliver IT services. Contracting techniques for cloud services have matured since the early 2010s and continue to evolve rapidly, supporting the deep digital transformation and emerging business patterns that the cloud is enabling. This white paper looks at these developments and aims to serve as a guide and checklist of key points and issues that cloud customers and cloud service providers (**CSPs**) will need to consider in contracting for cloud services.

2. **Enterprise computing is migrating quickly to the cloud**. An epic migration is now well underway in enterprise (large organisation) computing from 'on premise' – traditional IT infrastructure at the user's site – to 'in cloud' – accessing the public cloud, the more dedicated resources of the private cloud, and their hybrid cloud combination. This migration to the cloud compares with the migration a century ago of electricity generation and supply from the factory to the power station and grid. The cloud however has more facets as each layer of the IT stack – physical infrastructure; networking and security; servers and storage; operating systems and middleware; and hosted applications and apps - gets the cloud's 'as a Service' treatment. This migration is gathering pace quickly.

3. **Cloud's share of enterprise IT will rise from 15% in 2018 to 45% by 2026**. Research company IDC estimates that "60% of all IT infrastructure and 60–70% of all software, services and technology spending [will be cloud-based] by 2020".[1] In enterprise computing, open source IT research organisation Wikibon has aggregated the elements of traditional enterprise IT, compared them to the private cloud and the Infrastructure (**IaaS**), Platform (**PaaS**) and Software (**SaaS**) elements of the public cloud and projected them all forward to 2026. The result is Wikibon's forecast that the cloud's share of enterprise computing will grow from around 15% currently to 45% by 2026.[2] The chart at Figure 1 on the next page is derived from these projections.

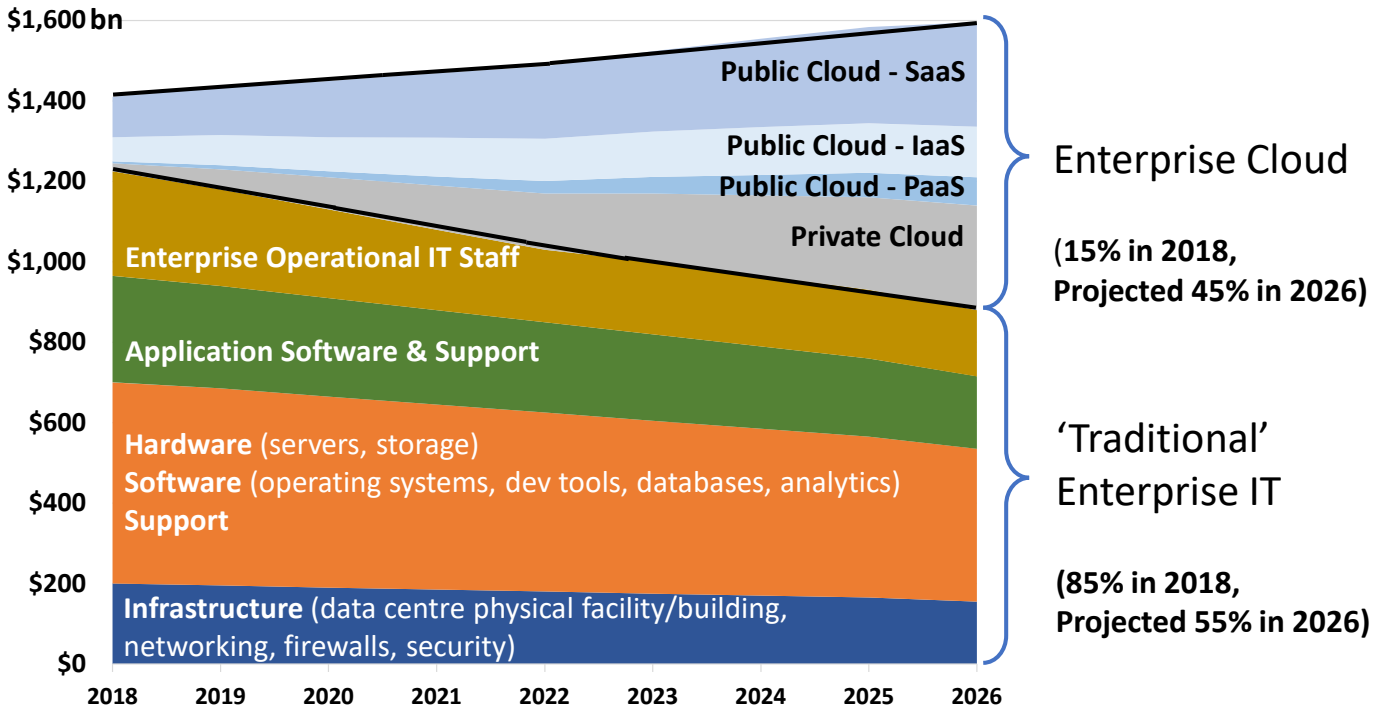
4. **Increasing data volumes are fuelling cloud growth**. The cloud, as an extension of Moore's Law, demonstrates the marvel of compound growth, and cloud data centre economics are truly mind boggling: driven by Internet of Things (**IoT**) sensors and social media, data volumes created are growing by 30% to 40% annually, so will increase by 4x to 5x over the next 5 years. Data created is currently two orders of magnitude (100x) higher than data stored, so data stored in the cloud has some catching up to do, and in 5 years' time will be 5x to

[1] Quoted in '*Four Trends in Cloud Computing CIOs Should Prepare For in 2019*', Asokan Ashok, Forbes, 5 July 2018 - https://www.forbes.com/sites/forbestechcouncil/2018/07/05/four-trends-in-cloud-computing-cios-should-prepare-for-in-2019/#702a1b544dc2

[2] '*Cloud "Vendor Revenue" Projections 2015-2016*', David Floyer, 28 February 2017, Wikibon - https://wikibon.com/cloud-vendor-revenue-projections-2015-2026/ - cited in '*Roundup of Cloud Computing Forecasts, 2017*', Louis Columbus, Forbes, April 29, 2017 - https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#253cc79331e8

10x higher than today.[3] At the same time, cloud power consumption rises[4] whilst everything inside the data centre gets smaller and faster: technology advances in cloud storage for example mean that storage device space - 'tin on the floor' - will reduce to a fraction of what it is today even as data volumes stored rise exponentially.

Figure 1: Worldwide Enterprise IT Projections by Segment (Traditional & Cloud) - 2018-2026 ($bn)



5. **Cloud Service Providers ('CSPs') are growing rapidly**. Today, there are around 500 hyperscale data centres globally,[5] and networking company Cisco Systems in its current Global Cloud Index forecasts that by 2021 this will rise to 628, operated by 24 CSPs and by then accounting for over 85% of the public cloud's installed server base and workloads.[6] The development of the cloud is particularly visible at the moment in the cloud

---

[3] See '*Data Age 2025*', ICD White Paper, April 2017 - https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

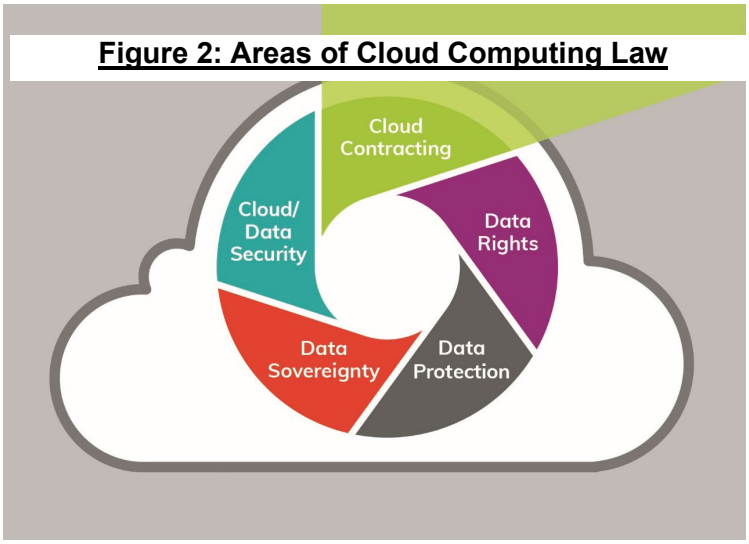
[4] Data centres are forecast to use between 1,200 TWh/year (terawatt hours per year) (best case) and 3500Twh/year (expected case) of electricity within 10 years, or between 4.5% and 13% of global electricity consumption. See '*Tsunami of data could consume one fifth of global electricity by 2025*', The Guardian, 11 December 2017 - https://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025 - citing '*Total Consumer Power Consumption Forecast*', Anders Andrae, 7 October 2017 - https://www.researchgate.net/publication/320225452_Total_Consumer_Power_Consumption_Forecast.

[5] There were estimated to be 430 hyperscale data centres at the end of 2018, with another 132 planned or under construction ('*Hyperscale Data Centre Numbers Increased by 11% in 2018*', Abigail Opiah, Data Economy, January 10, 2018 - https://data-economy.com/hyperscale-data-centre-numbers-increase-by-11-in-2018-report/

[6] '*Cisco Global Cloud Index: Forecast and Methodology, 2016-2021*' (updated November 2018) - https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html. Cisco defines criteria for hyperscale CSPs as annual revenues of (i) >$1bn from IaaS, PaaS or infrastructure hosting, (ii) >$2bn from SaaS, (iii) >$4bn from internet, search or social, or (iv) >$8bn from e-commerce or payment. Cisco identifies 24 hyperscale CSPs by these criteria, of which 17 are in the United States: Adobe, ADP, Amazon, Apple, AWS, eBay, Facebook, Google, IBM, Intuit, LinkedIn, Microsoft, Oracle, Rackspace, Salesforce, Twitter

revenue growth of the three largest CSPs, with Amazon Web Services (AWS) increasing by 50% annually and Microsoft and Google each by around 100%: by 2020, cloud revenues at AWS, Microsoft and Google are forecast to reach $44bn, $19bn and $17bn respectively.[7] This accelerating growth is driving economies of scale and declines in unit pricing, a key point for cloud buyers to watch out for, especially in longer term agreements.

6. **Areas of cloud computing law**. Contracting for cloud services is one of a number of rapidly evolving areas of cloud computing law. These areas overlap and may best be thought of as providing different perspectives and frameworks from which to analyse and assess cloud computing law issues. They may briefly be summarized as follows:



- ***cloud contracting***: the contract between the CSP and its customer;
- ***data rights***: the intellectual property and related rights arising around data stored and processed in the cloud;
- ***data protection***: the legal rights and duties arising around personal data in the context of the CSP's duties to the customer and the customer's wider data protection responsibilities;
- ***data sovereignty***: the extent to which the customer's data may be accessed in the cloud without its authorisation (or even knowledge) by the CSP or third parties (typically regulators and state agencies, frequently depending on the location of the data); and
- ***cloud/data security***: the legal, technical, operational and governance controls that an organisation puts in place to ensure desired cloud data security outcomes.

This white paper is one of an occasional series and focuses on contracting for cloud services. Further information on the other areas is provided in our white papers on Data Rights, Data Sovereignty and Cloud Security.[8] This white paper does not address specifically other areas of IT law that are developing under the umbrella of the fourth industrial revolution - like AI, autonomous vehicles, big data, blockchain, the IoT, robotics and digital transformation more generally – but as the scale, range and reach of cloud-based 'as a Service' offerings continues to proliferate, this paper touches on a number of them below in relation to their

---

and Yahoo; and 7 are elsewhere: Alibaba, Baidu, JD.com and Tencent (China); NTT and Yahoo! Japan (Japan); and SAP (Germany).

[7] '*Cloud Revenue 2020: Amazon's AWS $44B, Microsoft's Azure $18B, Google Cloud Platform $17B*', John Koetsier, Forbes, 30 April 2018 - https://www.forbes.com/sites/johnkoetsier/2018/04/30/cloud-revenue-2020-amazons-aws-44b-microsoft-azures-19b-google-cloud-platform-17b/2/#2d079dd11b43

[8] '*Legal Aspects of Managing Big Data*' (October 2014) - http://www.kempitlaw.com//wp-content/uploads/2014/10/Legal-Aspects-of-Big-Data-White-Paper-v2-1-October-2014.pdf; '*Cloud Computing and Data Sovereignty*' (March 2016) - http://www.kempitlaw.com/cloud-computing-and-data-sovereignty/; '*Legal Aspects of Cloud Computing: Cloud Security*' (June 2018) - http://www.kempitlaw.com/legal-aspects-of-cloud-computing-cloud-security/

cloud contracting aspects.[9]

7. **Aims and scope of this white paper**. The objective of this white paper is to provide by way of overview a guide and checklist of key points and issues that CSPs and their customers will need to consider in the cloud service contracting process. Its primary audience is the in-house lawyer at an organisation procuring cloud services from a CSP. Its secondary audience is in-house counsel at CSPs. It is written at 31 May 2019, from the perspective of English law. It is not legal advice. **Section B** describes characteristics of cloud computing and cloud contracts in more detail and contrasts the cloud with other IT contracts. **Sections C** to **G** focus on preparatory points (**C**), regulatory aspects (**D**), lifecycle issues (**E**), the more 'legal' points that arise (**F**), and emerging issues (**G**).

B. CHARACTERISTICS OF THE CLOUD AND CLOUD CONTRACTS

8. **The cloud: 5 characteristics, 3 service models, 4 deployment models**. The classic US NIST (National Institute of Standards and Technology) definition of cloud computing specifies a type of computing with five characteristics, three service models and four deployment models.[10]

9. **5 characteristics of the cloud.** The cloud's five key characteristics are:
   - ***on-demand self-service***: computing resources are obtained automatically as needed without direct CSP intervention;
   - ***broad network access***: computing resources are accessed through standard mechanisms anytime, anywhere;
   - ***resource pooling***: computing resources are pooled serving multiple customers on a multi-tenant basis;
   - ***rapid elasticity***: computing resources are scaled as needed so the customer can respond flexibly to demand; and
   - ***measured service***: computing resources consumption is monitored and controlled and the customer pays for resources used.

10. **3 service models of the cloud.** Figure 3 below shows the three primary service models of cloud computing, their constituent parts and how they interrelate. They are:
    - ***Infrastructure as a Service*** (***IaaS***): the lowest levels of the IT stack are provided from the cloud. Shown as levels 7, 6 and 5 in Figure 3, these are physical data centre, plus power and air conditioning; networking, firewalls and security; and compute (servers) and storage.

      IaaS is particularly suitable for test and development environments, website hosting, storage of large volumes of data, business continuity and disaster recovery functions and tasks requiring large amounts of computer power (big data analysis, etc). IaaS providers include AWS, Microsoft and Google (the three largest IaaS providers) and Rackspace, CenturyLink, IBM SoftLayer, Fujitsu, NTT, VMware and Virtustream.

---

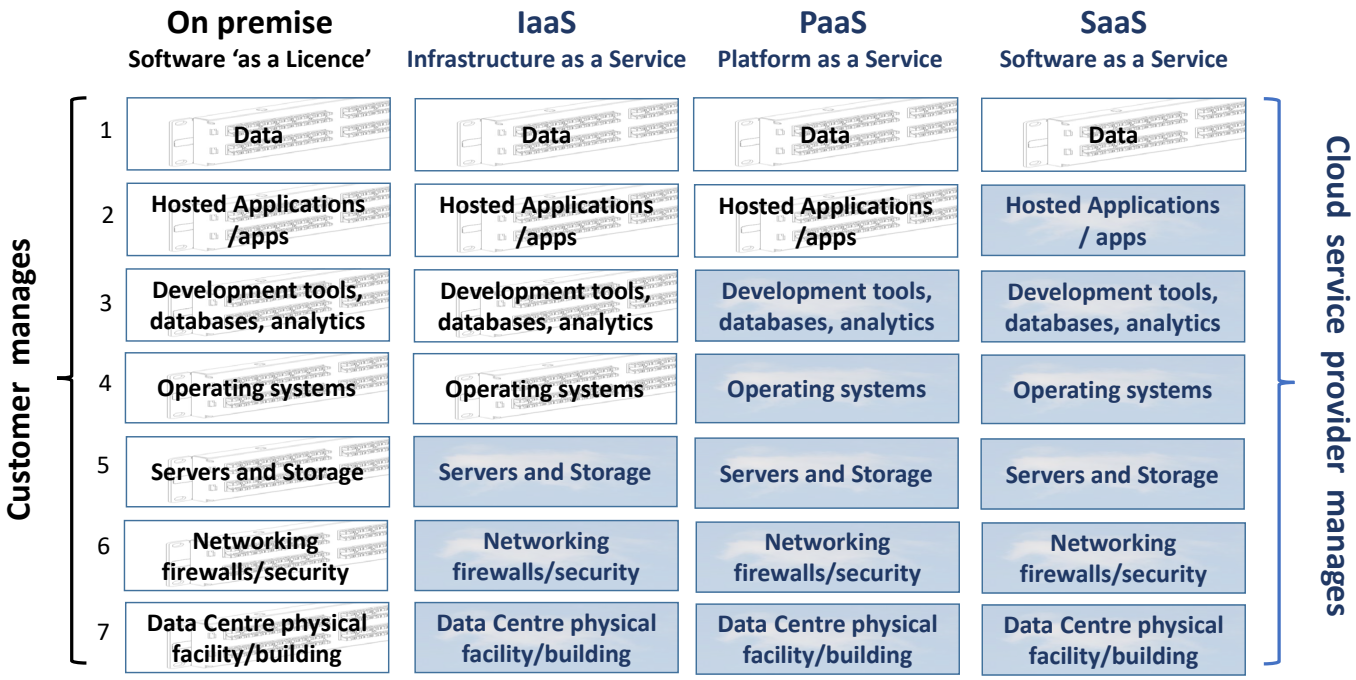
[9] For further information, see our white papers on '*Legal Aspects of Artificial Intelligence*' (September 2018) - http://www.kempitlaw.com/wp-content/uploads/2018/09/Legal-Aspects-of-AI-Kemp-IT-Law-v2.0-Sep-2018.pdf and '*Legal Aspects of the Internet of Things*' (June 2017) - http://www.kempitlaw.com/wp-content/uploads/2017/06/Legal-Aspects-of-the-Internet-of-Things-KITL-20170610.pdf

[10] '*The NIST Definition of Cloud Computing*', Peter Mell and Timothy Grance, September 2011 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- ***Platform as a Service*** (***PaaS***) – PaaS adds to IaaS operating system, database and analytics software, and development tools (levels 4 and 3 in Figure 3 below).

  PaaS is a platform whose components customers can use for the development or customisation of cloud-based applications. PaaS providers include AWS, Microsoft Azure, Google App Engine, Salesforce Platform, Red Hat Open Shirt, SAP HANNA Cloud Platform, Cloud Foundry and IBM Cloud.

Figure 3: Software 'as a Licence' to Software as a Service: the Cloud Service Continuum



- ***Software as a Service*** (***SaaS***) – SaaS adds hosted applications and apps to cloud provisioning (levels 2 and 1 in Figure 3 above). As the cloud develops and new services proliferate, it is now common to speak of XaaS ('Anything as a Service'). In addition to SaaS, examples include AIaaS (Artificial Intelligence), BPaaS (Business Process) and DaaS (as Data or Device).

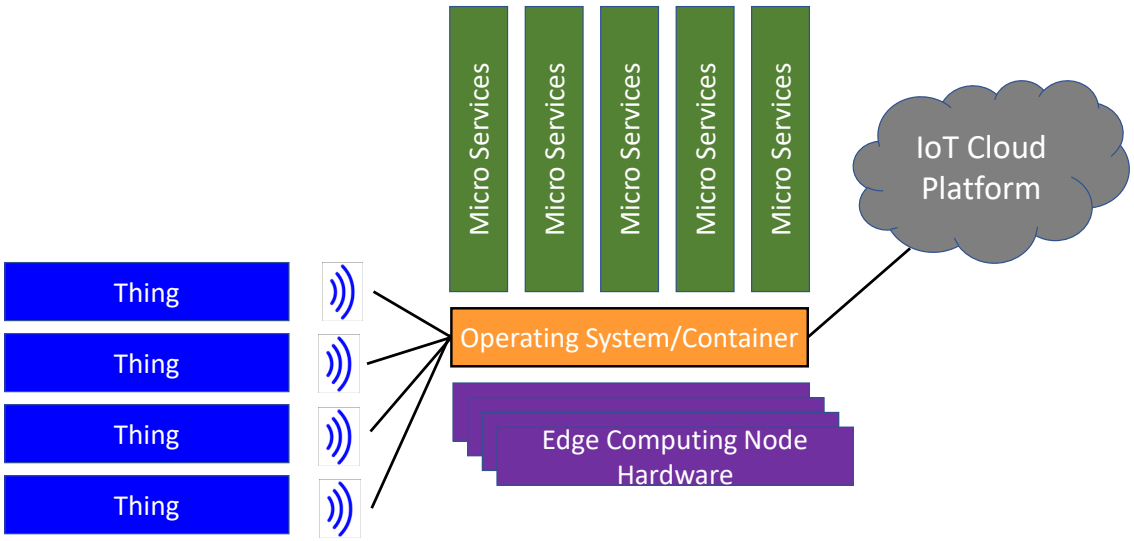
  Larger SaaS providers include Microsoft (Office 365), Google (G Suite), AWS SaaS, Adobe (editing and design), Dropbox (storage), Salesforce (CRM), Intuit (finance and tax), LogeMeIn (comms and conferencing), SAP (ERP), ServiceNow (service management) and Workday (HR).

11. **4 deployment models of the cloud**. The 4 main deployment models of cloud services are:
    - ***private cloud***: where infrastructure, platform or software are dedicated to one customer;
    - ***public cloud***: where service is provided to customers on a multi-tenant basis using shared infrastructure, platform or software and managed over the public Internet;
    - ***hybrid cloud***: as private cloud with access to public cloud to manage peaks; and
    - ***community cloud***: used by a community of customers rather than a single one.

12. **The gathering cloud: 'core', 'edge' 'microservices' and 'containers'**. As the cloud develops and extends, it is becoming increasingly common to speak of its 'core' and 'edge', and 'microservices' and 'containers'. Microservices and container boost the cloud's efficiency by enabling routine processing tasks to be carried out at the edge where the data is generated, avoiding the unnecessary journey to the core and back again (see Figure 4).

- the ***'core'*** is the cloud's engine room – the hyperscale and other data centres around the world that make up the cloud;
- the ***'edge'*** is where the cloud connects with the billions of IoT sensors and other devices at the edge of the physical world. Tuned by machine learning baked into the software that runs cloud operations and hunts for efficiencies, edge computing enables data generated by IoT and other devices to be more cheaply processed close to source and away from the core;[11]
- '***microservices***' are small, discrete, independently deployable applications designed to run anywhere and that carry the bare minimum resources to do a specific job.
- '***containers***' deliver microservices to and deploy them at the edge . More technically, containers are to OS (operating system) virtualisation what the hypervisor is to machine virtualisation. Unlike a VM (virtual machine), containers do not contain an operating system but call on OS resources via an API (application programming interface).

Figure 4: Edge Computing[12]



13. **Cloud contracts contrasted with outsourcing, software licence and professional services agreements**. Table 1 on the next page provides a high level, 'at a glance', view distinguishing cloud services agreements from outsourcing, software licence, and professional services agreements. Essentially, cloud services are generally provided on a 'one to many' basis (where a useful analogy is that the customer taking a room at the CSP's hotel) while outsourcing and professional services (typically implementation services) are provided 'one to one'. The essence of a software licence agreement is the grant of a licence of the copyright and other intellectual property rights ('**IPR**') in the software to permit use, whilst in cloud contracts, although access to the software being provided is licensed in IPR terms, service provision aspects tend to be at least equally important.

[11] See '*The future of computing is at the edge*', Richard Waters, Financial Times, 6 June 2018 - https://www.ft.com/content/1dba534a-5857-11e8-bdb7-f6677d2e1ce8

[12] See '*Edge Intelligence: The Central Cloud is Dead – Long Live the Edge Cloud!*" https://www.iiconsortium.org/news/joi-articles/2017-Sept-Edge_Intel_The_central_cloud_is_dead-long_live_edge_cloud_JOI.pdf. Thanks to Deirdre Moynihan at KITL for pointing out this graphic.

Table 1: Cloud contracts contrasted with outsourcing, software licence and professional services agreements

A. Issue		B. Cloud Agreement	C. Outsourcing Agreement	D. Software Licence Agreement	E. Professional Services Agreement
Provision basis:		**IT resources/functionality provided 'as a Service'**	**IT / process / function outsourcing service provision**	**IPR licence of rights in software + provision of maintenance services**	**provision of development / implementation services**
1	**Duration**	monthly, annually or fixed term	used to be longer term (e.g. 3, 5, 7 yrs) – now shorter	Perpetual: + annual maintenance; subscription: annual licence/main fee;	typically master services agreement (MSA) + individual statements of work (SOWs)
2	**Service standard**	'one to many' service as described – limited scope to change	'one to one' – service spec agreed upfront	conformance with spec	tied to key outcomes; reasonable skill & care; re-performance warranty
3	**SLA**	part of 'product' so limited scope to change	negotiated individually	part of support & maintenance terms	project based on & tied to key outcomes
4	**Time for performance**	24 x 7 availability subject to SLA	Part of SLA	part of SLA	based on project plan (implement) or devpt methodology (e.g. waterfall / agile / DevOps)
5	**Price**	subscription fee: by seat, resources consumed, subject to price change by CSP on notice or renewal	service charge agreed for duration of deal (e.g. annual fee) subject to change control, etc	perpetual: upfront licence fee + 20% maintenance p.a.; subscription: annual licence/maint fee;	fixed price: paid by milestone or other event T&M: fee rates agreed, invoiced monthly in arrears
6	**Data protection**	CSP likely (not always) to be data processor	provider may well be data controller	provider likely (not always) to be data processor	provider may well be a data controller
7	**Regulatory**	cloud equated to outsourcing under regulation in many sectors; TUPE unlikely to apply;	specific regulatory requirements apply in many sectors; TUPE likely to apply;	less intrusive regulatory environment where software is on prem; TUPE unlikely to apply;	certain specific regulatory requirements may apply, less intrusive than for outsourcing; consider whether TUPE may apply;

8	**Audit**	audit terms at least as required by customer's regulator and applicable law	audit right to monitor conformance vis a vis contract, regulator, other customers (MFN) and market (benchmark)	less need for audit right unless required by regulator or to monitor maintenance	audit terms as required by regulator and to monitor conformance with contract
9	**Liability limitation**	indirect loss excluded; direct loss lability limit: say 12-24 mths fees; limit may be higher for breach of IS, data protection or confidentiality obligations;	certain indirect loss may be included; liability limit generally set by reference to overall price; higher limit for certain kinds of breach;	indirect loss generally excluded; direct loss limit set by reference to contract value or maintenance fees after a certain time;	indirect loss generally excluded; direct loss limit: 150-200% overall fees; limit may be higher for breach of info security, data protection or confidentiality;
10	**Data rights, return**	Data return at contract end and (maybe) on demand; CSP gains no right to customer data;	contract to state customer's and providers' rights to data; return of data at contract end to customer or successor	if licensed software is on premises, data will generally not leave the building	provider access to data will be strictly controlled
11	**Termination**	generally no termination for convenience right on agreement duration >3 mths; data to be returned and exit assistance provided however termination arises; customer needs to manage lock-in risk;	generally no right to terminate for convenience; details of hand back to customer or over to successor need to be specifically addressed;	maintenance may be terminated on notice at end of year; consider what happens to data when software is de-installed;	may be termination for convenience right; consider IPR/confidentiality position post-term of deliverables generated during the contract;

14. **Evolution of cloud contracts**. Mass market apps and consumer services (including for example those available from the so-called 'FAANGs' - Facebook, Apple, Amazon, Netflix and Google) are provided from the cloud, under 'as is, where is' Terms of Service ('**ToS**') accepted by the user on a click-accept basis without any real opportunity to change.

    In the business cloud market, Kuan Hon, Millard and Walden writing in 2013 (so before the migration to the cloud had really got underway) perceptively noted a number of nascent trends:[13]

    > "The market, while becoming more sophisticated and transparent, may be fragmenting. There will be bigger providers offering general "one-size-fits-all" commodity services. However, niche providers and integrators are emerging who are more willing to tailor contract or service features to user needs. …
    >
    > Large providers are realising that … they must adapt: several global providers are offering different services with different pricings and terms … with specific terms for certain market sectors or functionality. …
    >
    > Large users who could require contracts on their own standard terms are making their terms cloud-friendlier. …
    >
    > With customised, managed private cloud services on dedicated infrastructure, providers may show more flexibility on contract terms. However, commoditised public cloud services on shared infrastructure are very different. They are cheap because of standardisation."

15. **Types of cloud contracts**. Since 2013, these trends have developed along the lines noted by the authors. Although CSPs can and do use a multiplicity of contract types for business cloud services, an evolving pattern for enterprise cloud contracting is emerging around a Master Software, Subscription and/or Services Agreement ('**MSA**') incorporating:

    - the particular subscription cloud services contracted for, typically under an Order Form ('**OF**'),
    - a Service Level Policy ('**SLP**') and Service Level Agreement ('**SLA**') as the performance yardstick for the services contracted;
    - a Statement of Work ('**SOW**') detailing the (configuration, customisation and implementation) professional services that the CSP contracts to provide so as to enable the cloud service; and
    - a Data Protection Addendum ('**DPA**') addressing privacy and information security requirements.

    Business to business cloud service provision has many contracting variants and the above pattern is by no means ubiquitous but it provides a convenient structure for the purpose of this white paper.

    As a practical matter, larger CSPs are increasingly standardising their contract terms for business customers and making them available through a website portal or otherwise online. The pattern is also to link through from the top level contract terms to (or 'nest') other sets of applicable terms (for example, specific terms applying to the growing range of individual services the CSP offers, generic use rights, SLAs, etc), which may themselves nest a third level (perhaps DPA and information security terms) and so on. The top level terms incorporate the various levels of nested terms by reference and may give extensive rights to change them. Customers should therefore make themselves aware of all the terms that apply to their agreement and makes sure in their contracts database that they have access at any time to all the then applicable terms.

---

[13] '*Cloud Computing Law*', ed. Millard, Oxford University Press, 2013 p.105

C. CLOUD CONTRACTING: PRE-CONTRACT POINTS

16. **Digital transformation and cloud migration routemap**. Cloud migration is an essential part of digital transformation. Successfully migrating processes, workloads and data to the cloud involves appreciating where on a spectrum of data sensitivity a particular application and the data it processes lie. This in turn means establishing a classification for workloads and datasets to ensure that the balance is correctly set between security, sensitivity, availability, cost and other relevant factors:

> "Data classification provides one of the most basic ways for organizations to determine and assign relative values to the data they possess. The process of data classification allows organizations to categorize their stored data by sensitivity and business impact in order to determine the risks associated with the data. After the process is completed, organizations can manage their data in ways that reflect its value to them instead of treating all data the same way. Data classification is a conscious, thoughtful approach that enables organizations to realize optimizations that might not be possible when all data is assigned the same value."[14]

Or, to put it another way, absence of data classification risks the customer paying the highest rate by default as all data will be treated as of the same value. Organisations should consider including data classification as part of the development of their structured, longer range plans mapping out all the relevant steps for their cloud migration in the context of their digital transformation journey.

17. **CSP pre-contract due diligence: general**. Carrying out pre-contract due diligence and taking credit and customer references for potential CSPs is critical for the customer. For larger cloud contracts, the customer should consider requiring each bidder in the competitive process to confirm that it will warrant in the contract that its responses to the statement of requirements in the Request for Proposal ('**RFP**') are true, accurate and complete if that bidder be selected.

18. **CSP pre-contract due diligence: information security assessment ('ISA')**. A particular feature of cloud contracts is the criticality of data or information security ('**IS**'). The regulatory aspects of IS relating to cloud contracts are reviewed further at paragraph **D.23** below, but the key point is that the customer will need to ensure that the CSP is able to provide an appropriate level of security for the workloads and data that the contract is to cover. The customer should therefore start preparing a written ISA at an early stage, effectively running in parallel with the process to let and negotiate the contract.

In the UK, the Government has done much of the heavy lifting from the cloud customer's perspective in this area, publishing in November 2018 fourteen principles for cloud security and how the UK public sector should consider implementing them.[15] These principles lend themselves to the private sector also. This ISA should cover (among other things) (i) where the data is to be hosted, (ii) details of data centre provider, (iii) type of hosting (dedicated/shared hardware/virtual server, private cloud, etc), (iv) details of network security and server configuration, (v) encryption arrangements, (vi) development testing and release management, (vii) access management, (viii) data retention, (ix) business continuity / disaster recovery and (x) incident

---

[14] '*Data Classification for Cloud Readiness*', Microsoft, 2014 - https://www.microsoft.com/en-us/search/result.aspx?q=data+classification+for+cloud+readiness

[15] '*Implementing the Cloud Security Principles*', National Cyber Security Centre ('**NCSC**'), November 2018 - https://www.ncsc.gov.uk/collection/cloud-security. For further detail, see our white paper on '*Legal Aspects of Cloud Computing: Cloud Security*' (June 2018) at pages 14 to 17 and the Annex - http://www.kempitlaw.com/legal-aspects-of-cloud-computing-cloud-security/

management.

19. **CSP pre-contract due diligence: information security assurance**. The customer will also need to consider how to evidence assurance that the CSP will be able to perform its IS commitments. This is done typically through a combination of warranted RFP responses, contractual commitments and evidence of third party standards certification, perhaps with independent testing for more critical aspects. Technical standards certification is emerging as a key part of the IS picture. The most commonly invoked security standards in cloud contracting at the moment are ISO/IEC 27001 (IS management systems)[16], SSAE 18, SOC 2 reporting (which evaluates an organisation's information systems relevant to security, availability, processing, integrity, confidentiality or privacy)[17] and the NCSC's Cyber Essentials and Cyber Essentials Plus.[18]

    The customer will also need to obtain responses to a range of questions in order to verify that the standards the CSP is invoking cover the services to be contracted. These questions include: (i) has the certificate been issued by an approved certifier? (ii) does it cover all aspects of the contracted CSP service? (iii) does it cover all data centres where customer data is to be stored? (iv) is it complete? (v) is it current? (vi) will the CSP commit to keep it current for the agreement term? (vii) if the CSP loses the committed certification, must it notify the customer promptly? (viii) can the customer terminate the agreement for CSP breach of any of these commitments?

20. **CSP pre-contract due diligence: data protection impact assessment ('DPIA')**. The regulatory aspects of data protection in cloud contracts are briefly overviewed at paragraph **D.22** below. The customer should consider whether it will need to prepare a DPIA and if so whether to start it at the due diligence pre-contract stage and prepare it in parallel with negotiating the contract.[19] Even where there is no regulatory requirement to prepare a DPIA, it is generally good practice to do so.

21. **CSP pre-contract due diligence: CSP-side dependencies**. One of the cloud's main features is the facilitation of faster service deployment and lower prices through the economies of scale and scope that aggregation of computing resources enables. A corollary of this is that a CSP may depend on other providers in order to deliver the contracted cloud service and so the customer may be at risk if service from any of these other providers, or the provider itself, fails. Cloud service provision has yet to go through one of the 'busts' that periodically affect the IT industry, but customers should be alert to supplier dependencies that may impact service integrity. The related point of obtaining visibility of the provider's sub-contractors and supply chain for data protection purposes (see paragraph **D.22** below) may assist the customer here.

---

[16] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[17] The **SSAE** (Statement on Standards for Attestation Engagements) is a US accountancy originating standard relating to auditing for service organisations. SSAE 16 (which entered into effect in 2011) was replaced by SSAE 18 in May 2017.

[18] Press Release, 26 September 2014, '*Government mandates new cyber security standards for suppliers*' (Procurement Policy Note 09/13 - https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers)

[19] See '*How do we do a DPIA*' (Information Commissioner's Office ('ICO') - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how2 and the sample DPIA template available there.

D. CLOUD CONTRACTING: REGULATORY ASPECTS

22. **Privacy and data protection**. The coming into force in May 2018 of the GDPR[20] (and in the UK, the Data Protection Act 2018)[21] marked a step change in privacy and personal data regulation with significant consequences for cloud contracting. The months following saw customers and CSPs alike looking to retrofit GDPR compliant contractual terms to pre-GDPR cloud contracts, leading to a 'battle of the forms', particularly between enterprise customers and large CSPs, as they each sought to apply their own terms across their contract estate. Since then, market practice appears to be evolving around the DPA (Data Protection Addendum) in standard form proposed by the CSP as a basis for incorporation into the main Cloud Agreement, which is then reviewed by the customer and may be negotiated between the parties. Although we do not review data protection law in detail here, where GDPR is relevant (which will almost always be the case where the service covered by the cloud contract touches personal data anywhere in the EU/UK) key questions include the following:

    i) ***Will the customer need to prepare a data protection impact assessment ('DPIA')?*** As mentioned at paragraph **C.20** above, the customer should consider at an early stage whether to prepare a DPIA for the cloud service and if so (whether required under GDPR or as good practice) to prepare it side by side with negotiating the contract.

    ii) ***Is the CSP a data controller or data processor?*** The GDPR sets out different codes depending on an entity's role as controller or processor of personal data.[22] The controller determines the purpose and means (the 'why' and 'how') of the processing, and has responsibilities arising *directly* under the GDPR. The processor processes personal data on behalf and on the instructions of the controller and is generally *indirectly* subject to the GDPR in this context through the controller's duty to have written terms in place with the processor.

    The position may be complex in practice as (i) the boundaries between controller and processor can be fuzzy; (ii) the same CSP can be a processor for some activities (e.g. SaaS provider) and a controller for others (e.g. professional services); (iii) if both are controllers, the customer and CSP may be separate controllers for some activities but joint controllers (where different duties arise) for others; and (iv) the CSP may also be providing personal data to the customer so GDPR may need to be addressed from both sides.

    iii) ***If data controller, what contract terms will need to be included?*** To the extent that the CSP is a data controller, the GDPR mandates no specific or prescriptive terms but the weight of the GDPR applies directly. However, contract terms normally include: (i) each of the customer and CSP accepting an obligation to the other to comply with the GDPR, etc; (ii) each accepting an obligation to cooperate with and assist the other on GDPR-related matters (the CSP may wish to put an annual cap on its assistance if provided without further charge); (iii) specific duties where the parties are joint controllers; (iv) an

---

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[21] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[22] Generally here see: '*Controllers and processors*' (ICO) - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/; *'Opinion 1/2010 on the concepts of 'controller' and 'processor''* (Art. 29 WP, Feb. 2010 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf; and '*Contracts and liabilities between controllers and processors*' (ICO draft guidance, Sept 2017) - https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

express obligation on the CSP to take appropriate technical and organisational measures for the security of personal data received from the customer, and a description of what these are; and (v) express obligations on the customer as regards GDPR compliance in relation both to the personal data it transfers to and receives from the CSP.

iv) ***If data processor, what contract terms will need to be included?*** Where the CSP is a processor, the GDPR elevated written contracts from a way of demonstrating compliance with the seventh data protection principle (appropriate technical measures) under the pre-GDPR law to a more prescriptive requirement to include the specific terms set out in GDPR Articles 28(3)(a) to (h), etc. Very briefly these are duties on the processor:

a) only to process personal data on the controller's written instructions (28(3)(a));

b) to ensure those authorised to process personal data are bound by secrecy (28(3)(b));

c) to implement appropriate technical and organisational measures ('**ATOM**') to manage processing security and risks (28(3)(c) and 32);

d) to identify sub-processors and flow down its duties to them (28(3)(d), 28(2) and 28(4));

e) to assist the controller in complying with data subject rights through ATOM (28(3)(e));

f) to assist the controller in complying with controller's security duties (28(3)(f), 32–36);

g) at the controller's option, to delete or return all personal data at service end (28(3)(g); and

h) to provide the controller with the information necessary to demonstrate compliance with its duties and allow for audits by the controller or its nominee (28(3)(h)).

In addition, the written terms should describe the scope, nature, purpose and duration of the processing, the types of personal data processed and the categories of data subject involved.

v) ***In each case what is the relationship between data protection and IS terms?*** GDPR duties in relation to IS are a subset of the IS duties that apply to cloud customers and CSPs more generally. Under the GDPR, they mainly arise (for controllers) directly under Articles 32 to 36 and (for processors) indirectly under Articles 28(3)(c) (calling down Article 32) and 28(3)(f) (calling down Articles 32 to 36). See also paragraphs **C.18**, **C.19** and **C.20** above.

vi) ***In each case will personal data be exported from the UK/EU?*** Articles 44 to 50 GDPR cover transfers of personal data to countries outside the EU. Broadly, for any third country where the EU has not taken an 'adequacy' decision on the privacy laws of that country, data exports are permitted only (i) where the entities have entered into Binding Corporate Rules ('**BCRs**') regarding personal data, (ii) (in the case of transfer to the US) where Privacy Shield arrangements apply, or (iii) where the parties have entered into so-called standard contractual clauses (controller to controller flavour, or controller to processor flavour).[23] Where the CSP is a data processor and personal data is to be processed outside the adequacy, BCR or Privacy Shield regimes, effectively two sets of controller to processor clauses will need to be included in the cloud contract: first, those prescribed by Article 28; and second, the standard contractual clauses (controller to processor). Where the CSP is a data controller and adequacy, BCR or Privacy Shield

[23] See '*Standard Contractual Clauses (SCC) – standard contractual clauses for data transfers between EU and non-EU countries*', European Commission - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

arrangements do not apply, the standard clauses (controller to controller) will be needed.

vii) ***In each case, what audit rights will the customer or its regulator have?*** Where the CSP is a data processor, Article 28(3)(h) requires the processor to:

> "make available all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."

In the context of cloud computing, this can lead to practical difficulties, especially over audits and inspections where access to the host data centre is restricted (in compliance with the CSP's own processes and security duties). Nonetheless, the customer should insist on this requirement, not only as regards the customer's data protection regulator but also in regulated sectors where the cloud service is equated to outsourcing and/or subject to audit or inspection by the customer's sector regulator;

viii) ***What is the liability position for breach of data protection obligations?*** Liability under the GDPR may arise under Article 83 through fines imposed by the regulator (which may be substantial – €10m or 2% of worldwide turnover, rising in certain cases to €20m or 4%) and under Article 82 through an award of damages to an injured third party who can prove their loss. Articles 82(1) and (2) provide as follows:

> "1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
>
> 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

Articles 82 and 83 explain why discussions around the liability limitation clause in cloud contract have become more animated after May 2018. Market practice in enterprise cloud agreements is starting to develop around a contractual liability limitation construct where breach of the CSP's data protection, IS and confidentiality duties are removed from the general liability cap and dealt with separately, with either unlimited liability, a higher cap or indemnification, which may also cover fines and the costs of regulatory action. Please see also paragraph **F.42** below.

23. **Information security**. In addition to data protection, cloud customers and CSPs alike are subject to a wide range of generally applicable legal duties relating to IS which may impact cloud services contracts. We do not consider these in detail here[24] but overview in the following two tables key areas of law and how duties may arise:

Table 2: Sources of generally applicable enterprise-related information security UK legal duties

	Source	Brief description
UK criminal law		
1	Computer Misuse Act 1990	hacking, phishing, denial of service, malware attacks outlawed

[24] For further information, see our white paper on '*Legal Aspects of Cloud Computing: Cloud Security*', June 2018 - http://www.kempitlaw.com/legal-aspects-of-cloud-computing-cloud-security/

	Source	Brief description
2	UK Terrorism Acts 2000-2015	introduces terrorism offences in relation to cybersecurity
3	UK Fraud Act 2006	identity theft and phishing criminalised
Data protection, sovereignty and security		
4	GDPR/Data Protection Act 2018	see paragraphs **C.20** and **D.22** above
5	Data residency and location	see paragraph **D.25** below
6	Investigatory Powers Act 2016	regulates powers to intercept communications and to access and retain communications data
7	EU Cybersecurity Act[25]	regulation (coming into effect on 27 June 2019) to institutionalise ENISA and create an EU-wide cybersecurity framework for ICT
General and civil law		
8	Companies Act 2006 and UK Financial Conduct Authority ('**FCA**') requirements	duties of directors of private and public companies and FCA powers over companies and individuals under Financial Services and Markets Act 2000 ('**FSMA**')
9	Litigation	duties to the court relating to document discovery
10	Tort – negligence	duty to take reasonable care likely to be coextensive with duty to take appropriate technical and organisational measures
11	Misuse of private information, conversion, deceit, trespass	torts each separate from breach of GDPR
12	Breach of confidence, IPR infringement	software and data, etc protectible by law of confidence, copyright, database right, etc.
13	Breach of contract	as between contracting parties

Table 3: Sources of additional UK sector-specific enterprise-related information security legal duties

	Source	Brief description
Telecoms		
14	NIS Directive and UK implementing regs	applies to providers of cloud computing services (**CCS**) in the UK as relevant digital service providers (**RDSPs**) imposing security and other measures in relation to their CCS
15	Communications Act 2003, ss. 105(A) and 105(B)	public electronic communications network (**PECNs**) and public electronic communications service (**PECS**) providers must take technical and organisational

[25] Regulation EU 2019/881 of 17 April 2019 on ENISA (EU agency for cybersecurity) and information and communications technology cybersecurity certification (OJ L/151/15 of 7 June 2019, coming into force 27 June 2019 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

	Source	Brief description
		measures appropriately to manage risks to the security of their PECNs and PECSs
16	Privacy and E-communications Regulations 2003	PECS providers to take appropriate technical & organisational measures proportionate to the risks to safeguard the security of the service, whether alone or with PECN provider it uses
Financial Services		
17	FCA Handbook, MiFID/SYSC and outsourcing	FCA regulated organisations are subject to the FCA Handbook, including Principles for Business (**PRIN**), the Senior Management Arrangements Systems and Controls (**SYSC**) and Disclosure and Transparency Rules (**DTR**)
18	SMCR	SMCR will extends individual accountability within regulated FS organisations to all FSMA regulated firms from December 2019
19	FCA Cloud Guidance 2016	cloud services effectively equated with outsourcing and given green light as such by FCA
20	European Banking Authority ('**EBA**') recommendations on outsourcing to CSPs 2017	non-binding recommendations to be taken into account by FS organisations when outsourcing to CSPs, effective from July 2018
Government		
21	Official Secrets Acts 1911-1989	applies to Crown servants and UK government contractors and creates offences for disclosing (or failing to secure) information damaging to UK's interests
22	Freedom of Information Act 2000	Imposes disclosure obligations on government authorities and public sector organisations in certain circumstances
Healthcare		
23	reporting guidelines issues by central government	
24	Abortion Regulations 1991; Health Service (Control of Patient Information) Regulations 2002; Human Fertilisation & Embryology (Disclosure of Information for Research) Regulations 2010;	regulations set out when information about individuals can be processed for medical research and the safeguards that must be in place

24. **Sector specific regulation**. Specific regulation applies in a number of sectors, extending beyond data protection and IS to cover other areas also. Table 3 above illustrates these for the telecoms, financial services, public and healthcare sector. Other sectors with their own regulators – like the Solicitors Regulation Authority for legal services – will also generally look to have some oversight of their charges' cloud services. Here the

general pattern is to equate cloud services with outsourcing and regulatory power to audit and review if need be (despite the practical difficulties of enforcement).

25. **Data residency, location and sovereignty**. Greater data regulation and growing apprehension of 'data nationalism' are focusing customers' minds on where their data is to be stored and processed. In addition to the EU, other countries that have adopted data residency or export restriction requirements include Argentina, Australia, Canada, India, Israel, Malaysia, Mexico, Singapore, South Africa, South Korea, Switzerland and Uruguay. These concerns are leading increasingly to business deciding to use cloud services at a data centre located only in a particular country (perhaps the organisation's home state), and to require the CSP (i) to carry out processing only at the named data centre in that country, (ii) to ensure that the data remains resident there and (iii) not to transfer or transit it anywhere else (for example through account management, metadata, traffic data, sub-contracting or business continuity or disaster recovery). CSPs are in turn responding to these customer choices by expanding the range of services, commitments and associated pricing that they offer. Customers seeking enforceable commitments on these points should carry out appropriate pre-contractual due diligence at the IS Assessment stage.

    Whilst data residency and location relate to the data itself as a digital asset, data sovereignty is a person's right to control disclosure of and access to their own data or data under their control. In cloud contracting, the customer needs to be aware of how and when their data in the cloud can be accessed by third parties and to be vigilant in contract negotiations on these points.

    The preceding paragraphs have addressed data protection, IS and other duties that arise in the cloud around the customer's data. Paragraph **E.31** below looks at the contractual aspects of what the CSP may do with the customer's data. In addition, in the UK and under the Investigatory Powers Act 2016 ('**IPA**'),[26] the security services may, by warrant or other authorisation, intercept communications (i.e. monitor or collect the content of a message in the course of transmission) and gather communications data (essentially, everything about a message other than its content), in certain cases without notifying the CSP or the customer. The customer should seek clarity in the contract around the extent to which its right to control access to and disclosure of its data in the cloud is subject to exceptions, what those exceptions are and what they mean.

26. **The international context – governing law and jurisdiction**. The cloud customer will generally want the cloud contract to be governed by the law of its home state (the law of England and Wales, Scotland or Northern Ireland where the customer is based in the UK). Larger CSPs may be willing to accommodate this, particularly if they have UK based operations, but smaller CSPs based outside the UK may seek to have their own country's or state's laws apply. From the UK customer's point of view, risk is reduced by having UK law apply, particularly where the UK courts have exclusive jurisdiction to hear any disputes. If the CSP is based outside the UK and EU and is insistent on its home law applying, the customer should be aware of the difficulties that this may cause. The situation may become complex where non-excludable regulatory law (for example the GDPR) applies in non-UK/EU proceedings alongside the home law of the CSP. Here, evidence about the GDPR or other UK regulation concerned will generally be adduced before the overseas court as evidence of fact based on what each party's third party experts say rather than of law argued by the parties' lawyers. Because of the cost, duration and impact of litigation, it is increasingly the case that the parties agree to informal internal dispute resolution, generally escalating through two or three levels inside the parties' organisations before having resort to the courts.

[26] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

E. CLOUD CONTRACTING: LIFECYCLE ISSUES

27. **Professional services**. For many cloud services a degree of implementation or configuration services – as professional services – may be necessary before the cloud services themselves may be used. Such services are generally provided either by the CSP under a SOW separate from the cloud services themselves but still under the generic MSA or by a third party implementation services provider under a separate agreement. In either case the contracting basis for these professional services is generally rather different than from the cloud services themselves – see column E of Table 1 at paragraph **B.14** above.

28. **Service standards and the SLA: availability, response times and incident management**. In cloud contracting, the service standards and Service Level Agreement ('**SLA**') that the CSP commits to are effectively part of the product that the CSP is delivering on the cloud's 'one to many' basis. This means the SLA that the CSP offers should be considered pre-contract as part of due diligence as the scope for negotiating better terms (even in practice in the private cloud) is likely to be limited.

    The CSP may commit that the cloud service will comply with the service description, and in that case the customer should check carefully whether the service description is too vague or, equally, too detailed to be actionable. This puts more weight on to the express cloud service levels, which will generally be of two types: first, as to service *availability* (where the service level will very often be above 99.5% over the reference period, subject to periods of scheduled maintenance) and service *response* (where the service level will generally be a proportion of transactions returned in a certain number of seconds or less); and second as to *incident management* (support and maintenance), which normally follow market practice based on a three or four level grid of issue severity by reference to time to respond and time to fix.

    For the first type (service availability and transaction response), the CSP will likely offer service credits, rising if service level defaults recur in months two and three after the first month. For the second type, the CSP may offer committed issue response times and that the issue if not resolved may be escalated through the parties' organisations, but generally (as in on-premises software licensing) will be reticent about committing a time to fix.

    Especially for the service availability and transaction response service levels, the customer may consider negotiating into the contract that for service level defaults occurring in, say, four consecutive months or four months in any 12, it has an express right to terminate for the CSP's breach (without a right for the CSP to remedy the breach) and claim damages. Such a right would need to be exercised carefully bearing in mind the time that will be necessary to switch to an alternative provider.

29. **Integration**. Increasingly with cloud software services as with on premises software licences, the contracted functionality will be communicating with a range of other software systems. As the range and extent of available cloud services expands, the same issues as to licence scope that have arisen in the traditional software licensing area are therefore likely to arise in the field of cloud services and contracting, and the customer should be aware of the risks of over-deployment.[27]

[27] In the on-premises software licensing area, see '*SAP v Diageo – the U.K.'s first software over-deployment case: takeaways for business*', Deirdre Moynihan, March 2017 - http://www.kempitlaw.com/sap-v-diageo-the-uks-first-software-over-deployment-case-takeaways-for-business/

30. **Customer-side dependencies**. Complex dependencies may arise where customers deploy multiple cloud services. For example, retailers going through digital transformation are looking to software systems increasingly sourced from the cloud to manage product information, digital assets, web content, digital experience, customer relationship and data analytics. What happens if one of these implementations is late, or if the cloud platform goes down, and how would loss of the PIM – the product information system that typically feeds web content, digital experience and CRM in retail – affect the other services? The customer will need to consider these aspects in terms of project management and governance (where the systems implementer or integrator will have a big role) and relief events (the CSP's 'get out of jail free' card if a delay not of its own making moves things right). The customer should consider having a 'one size fits all' project management/governance schedule that it applies in each contract with its CSPs and integration and implementation service partners.

31. **Data integrity: recovery and retention**. As we have seen, the CSP's duties in relation to the data processed by the service will overlap with the parties' contractual and regulatory data protection and IS obligations. The provider will generally seek to limit or even exclude liability for loss or destruction of data. This may be negotiable to an extent but the customer should bear in mind from the outset all aspects of data risk, covering this off in the DPIA (in relation to security of personal data), the ISA and the IS assurance it seeks. Particular emphasis should be placed on the extent to which the CSP will commit contractually to take 'appropriate technical and organisational measures' ('**ATOM**') and the contractual description of those measures, to ensure the security of the information processed.

    Other key questions include: (i) can the data in the cloud be backed up elsewhere, or is the CSP effectively the only person with possession? (ii) can the CSP make use, independently of the service, of any of the customer's data or data derived from it? (iii) does the customer own all IPR in and to (a) the data it uploads, (b) the data as processed, (c) service data, (d) metadata ('data about data') and (e) derived data? (iv) can the customer, at any time during the contract lifecycle as well as at its end, download the data? (v) is the data easily downloadable in an industry recognised format that is ready for the customer or an alternative provider to use? and (vi) what are the arrangements for return or destruction of data at contract end?

32. **Pricing**. Cloud pricing is generally on a subscription basis by time (monthly, quarterly, annually or longer fixed term) and seats (number of individual users). Except for monthly contracts, the CSP may seek to limit the extent to which customers can reduce the number of contracted seats as a way of reducing the initial commitment on which contract pricing was based. Business customers may well be able to fix the price for the initial contract term, but should also consider trying to fix pricing for renewal terms or at least capping any increase on a 'not to exceed' basis to reduce lock-in.

33. **Managing change**. As public, and to an extent private, cloud service is provided on a multi-tenant basis, the CSP will generally be improving and updating its service over the contract lifecycle and will want to make sure in the MSA that it preserves flexibility to do so. The customer will get the benefit of this through its subscription fee (which effectively wraps up into one the licence and support and maintenance fees charged separately in an on-premise licence, and adds in the hosting/service charge element). However, the customer should consider negotiating a term to make sure that no service improvements or updates will have the effect of removing compatibility or interoperability with other services that the customer was counting on as being able to work with the cloud service during contract lifecycle.

34. **Contracting for group companies**. Where the customer is contracting for service that is to be delivered to other group companies, it should consider how this is to be achieved, as it will generally not want each group

company receiving service to be a party to the agreement. The CSP however will want to make sure that it has recourse to the customer in the event that an affiliate breaches the agreement. From the customer's perspective, this can be achieved by expressly stating that (i) the agreement and service provided are for the benefit of the customer and its other group companies, (ii) acts and omissions by any other group company are treated as acts and omissions of the contracting customer, but (iii) the customer's obligations are not to be treated as obligations of other group companies where they are not named parties to the agreement.

35. **Responsibility for authorised users**. In the case of agreements that are not signed by each party at the start of the relationship but are brought into effect through click wrap acceptance by individual customer authorised users, contract formation difficulties will arise where the person click wrapping acceptance does not have authority to bind the customer.

    The customer will generally be expected to commit to manage authorised users starting with and leaving the customer's employment to ensure that seat limits are not exceeded (or if they are that the customer will pay any excess charges) and to ensure that its authorised users comply with express obligations around password and service use security. The customer should ensure it is in a position to effectively monitor and operate any CSP requirements in these areas. The CSP may seek to apply an Acceptable Use Policy, and if so the customer should review this to ensure that it does not overreach for the service concerned.

36. **Term, suspension and termination**. The customer should review all paths to termination in the contract. The CSP will normally seek to provide that failure within, say, 30 days to comply with a breach notice requiring payment to be made grounds termination for the customer's breach and insist that breach of the customer's payment obligations stand outside the limitation of liability. The customer should limit this to failure to pay 'undisputed' amounts and consider a longer cure period. The CSP may also look to build in a right to suspend service whenever the customer is in breach of payment obligations, and any service suspension right should generally be resisted by the customer.

    Longer terms cloud contracts can come with a sting in the tail. There is naturally a trade-off between price and duration but if the customer chooses a longer deal for a better price, then it will generally have no right to walk away and terminate for convenience part way through. The CSP's MSA will generally say if the contract ends through the customer's breach that the customer still has to pay all the charges for the balance of the term. The customer should consider resisting this and ideally get the vendor to claim damages for breach of contract and prove its recoverable loss in the usual way; or, failing that, contractualise the CSP's 'duty' that arises under general contract law to mitigate its loss (really, a requirement to take reasonable steps to reduce the impact of the breach); or negotiate a percentage discount off the remaining charges and state that payment is the vendor's only remedy so that the CSP is not able to use the customer's payment to fund a damages claim if its loss is greater than the early payment amount.

37. **Lock-in and exit**. Although ease of use and speed of deployment are particular features of the cloud, the customer should consider the extent to which lock in and switching suppliers may be an issue in practice. The customer should consider putting in place an express disengagement plan engaging the CSP's resources, whatever the reason for termination, to play 'nice' and assist the customer and any replacement provider in handing back/over the service it was providing. Ideally, the exit plan should be agreed within a short period (say 3 months) of the service start date and be reviewed annually through contract lifecycle. The customer should also ensure, if the CSP has a right to serve notice to terminate at the initial or a renewal term end, that the period of notice is sufficient to enable it to switch sourcing. The points about return of data (paragraph **D.31** above) and termination payments (**D.36**) are also relevant here.

F. CLOUD CONTRACTING: THE 'LEGALS'

38. **Express obligations to comply with law and customer policies**. Most MSA's will include a term that each party agrees with the other to comply with all applicable law (whether or not that is defined). The CSP may contend that it is not therefore necessary to include more detailed or granular obligations to comply with a particular law. We have seen above how in the case of data protection controller to processor clauses, the GDPR mandates prescriptive terms to be included in the contract and how the duty to take 'ATOM' (appropriate technical and organisational measures) in relation to IS is again more specific. In general terms, the customer is better protected by more, specific compliance with law duties on the part of the CSP.

    The customer may also wish to ensure that the CSP complies with its applicable policies. This is particularly the case in regulated sectors like financial services and healthcare. A practical difficulty is that the CSP may find it difficult on its multitenant model to accept obligations to comply with policy requirements of particular customers. However, as cloud provision becomes more extensive and CSPs offer more services that comply with particular sector specific regulatory requirements, market practice is emerging around (i) the CSP agreeing to comply with customer policies provided before contract start, (ii) the CSP accepting new or certain changes to customer policies on a chargeable basis through change control; (iii) more generally, in terms of regulatory support, the CSP agreeing to provide a certain number of hours' assistance each year without further charge (unless the reason for the assistance is CSP breach), charging for excess time at an agreed rate.

39. **Intellectual property rights ('IPR')**. IPR is of central importance to cloud operations, particularly in the areas of patent infringement, software copyright and IPR in relation to data.

    Cloud software has always been an easy target for patent infringement claims from NPEs (non-practising entities, businesses that buy patents to sue others for infringement as their only revenue source). This is why patent statistics consistently show increased NPE cloud activity over the last five years, as NPEs acquire patents (acquisitions grew from 69 to 540 between 2014 and 2018), engage in litigation (NPEs launched 200 cloud lawsuits in 2018, up from 120 in 2015), and recover damages (median damages awards were 3.5 times higher for NPEs than other claimants between 2013 and 2017). In response, some CSPs are providing contractual cover to customers in the form of IPR indemnities to cover patent claims.[28]

    Cloud use of software can invoke copyright in a number of ways. If the CSP's software is downloaded to the authorised user's machine or the customer's server, this will involve copying the software and so required the licence of the copyright owner (generally but not always the CSP). Cloud software copyright questions may be complex where the CSP's GUI (graphical user interface), APIs (application programming interfaces) or other elements of the CSP's software are downloaded to the user's browser or otherwise made available to the customer. This is why CSP agreement normally take a similar approach to copyright licensing,

[28] See the following articles by Richard Kemp and Nooreen Ajmal: (i) '*Growing Patent Claim Risks in Cloud Computing*', June 2017 - http://www.kempitlaw.com/growing-patent-claim-risks-in-cloud-computing/; (ii) '*Cloud Patent Claim Risks and Cloud Service Providers' Evolving Contractual Responses*', August 2017 - http://www.kempitlaw.com/cloud-patent-claim-risks-and-cloud-service-providers-evolving-contractual-responses/; (iii) '*Azure IP Advantage in China: Towards 'Quiet Enjoyment' in the Global Cloud*?', October 2017 - http://www.kempitlaw.com/azure-ip-advantage-in-china-towards-quiet-enjoyment-in-the-global-cloud/; (iv) '*Cloud IP Litigation: Evolving Patent Defensive Counter Measures*', July 2018 - http://www.kempitlaw.com/cloud-ip-litigation-evolving-patent-defensive-counter-measures/; and (v) '*Reducing Patent Risks at the Edge*', April 2019 - http://www.kempitlaw.com/reducing-patent-risks-at-the-edge/.

(particularly) customer restrictions and indemnities (see paragraph **E.41** below) as on-premises software licences. Cloud use of open source software with copyleft (inheritance) requirements, such as under the Affero licence of the FSF (Free Software Foundation), may also require analysis.[29]

IPR in relation to data is currently developing rapidly. Although there are no rights ***in*** data, IPR – typically for cloud purposes, copyright, database right and rights of confidence – arise ***in relation to*** data. As mentioned at paragraph **E.31**, the customer will want the CPS's acknowledgement that the customer owns all IPR in and to the data it uploads, the data as processed, service data, metadata and derived data; and to bar the CSP from using that data outside the service. In addition to GDPR commitments, the CSP is likely to seek a warranty that the customer owns all IPR in and to the data it uploads and may seek indemnity cover in the event of a third party claim and for breach of contract.

40. **Confidentiality**. The customer will want to impose strict secrecy duties on the CSP and its staff managing the service. The confidentiality obligations in the MSA tie into but arise separately from the data protection and ISO duties reviewed above. This is why liability for breach of confidence, data protection and ISO obligations tend to get treated differently in the liability limitation clause and bunched together under a separate, higher, liability cap.

41. **Indemnities**. Indemnities have historically been more accepted in practice in the USA than the UK but are becoming more common here. In contract law terms, indemnities are an obligation to reimburse in certain circumstances and have more in common with paying a debt than with damages for breach of contract. In the UK, the main advantages of an indemnity claim over a breach of contract claim are that there is generally no requirement to prove loss; and legal fees may be recovered on a £ for £ basis, rather than as taxed costs (typically two thirds) as in a contract breach claim (where, again as distinct from US litigation, the losing party has to pay the taxed costs of the winning party).

    In cloud MSAs, the customer will generally seek a warranty that the CSP's software and technology does not infringe third party IPR and also indemnity cover in the event of a third party IPR infringement claim, which may extend to cover breach of the IPR warranty as well. The CSP may accept that its IPR indemnity is unlimited but will frequently wish to include a right to terminate the agreement on notice if it is unable to negotiate a work round to the infringement claim, which may leave the customer with residual risk unless warranty cover applies in that case. The CSP is also likely to seek indemnity cover against the customer's data or content infringing third party IPR.

42. **Liability**. As in most IT contracts, liability clauses are very often the last point to be agreed in a cloud MSA negotiation as this is where both sides' balancing of cost, benefit and risk are mediated. In business and enterprise cloud deals, market practice appears to be emerging around four points.

    First, the areas where the law prevents liability limitation or exclusion - negligence liability for death or personal injury, fraud and fraudulent misrepresentation – or that the parties agree not to exclude or limit – like wilful default, breach of the customer's payment obligations and sometimes (as mentioned at paragraph **F.41** above) liability under indemnities or breach of contract for intellectual property infringement. Second, acceptance that liability for consequential loss is excluded except in certain cases. Third, a general cap on remaining liability (i.e. direct loss) by references to annual charges, typically in a longer term agreement between 12 and 24 months charges. Fourth, an exception to the general cap in the case of liability for breach

[29] https://www.gnu.org/licenses/agpl-3.0.en.html

of contract obligations relating to confidentiality, GDPR and IS. This reflects a different balance to the general cap, where the risk to the customer is appreciably greater. Here there can be a higher cap on liability, frequently double the amount of the general cap, so between 24 and 48 months charges.

43. **Insurance**. Finally in this section, it is good practice for the customer to negotiate a contractual requirement for the CSP to carry sufficient insurance to cover the CSP's liability under the MSA. Generally speaking, market practice is moving in the direction of CSPs accepting this requirement.

G. CLOUD CONTRACTING: EMERGING ISSUES

44. **Migrating from on premises to in cloud during lifecycle**. Many organisations are currently procuring core software systems on an on premises, as a licence basis with a budgeted anticipated lifecycle of between five and ten years. System costs are typically (i) software charges on a perpetual licence fee basis, payable upfront; (ii) implementation and other professional services, payable monthly in arrears; and (iii) support and maintenance fees, payable annually at a rate of around 20% of the initial software licence cost. The customer will write these costs down over the lifecycle. However, cloud take-up means that many of these systems will become generally available in the cloud during this period. Customers procuring these systems now should therefore consider the issue of in-flight cloud migration during the budgeted lifecycle.

    Financially, this means marrying on premises pricing with cloud pricing. Cloud services are generally charged on an annual subscription basis (effectively rolling up licence with support and maintenance charges and adding cloud infrastructure costs) so the customer thinking of migrating part way through should consider agreeing upfront a term in the contract that it will pay no more for the software and maintenance in cloud for the balance of the contract than it would have done had the on-premises solution continued over the normal lifecycle. Where software licence fees are paid upfront, this in practice means negotiating that the annual SaaS fees are not more than the annual support and maintenance charge for the on premise software.

    The customer's rationale is that it is getting no greater economic benefit in the cloud from the SaaS than on premises from the perpetual licence so should not have to pay more for the software licence and support and maintenance charges. The customer may also need to factor in an allowance for the cloud infrastructure (hosting) charges on an annual basis, and will also need to budget for the additional professional services charges that will be necessary in planning and executing the migration itself.

45. **Contracting for AI services in the cloud**.[30] The vast computing resources of the cloud are increasingly being used by the large CSPs as a vehicle for their artificial intelligence (**AI**) and machine learning (**ML**) services. AIaaS is becoming an increasingly important cloud service - for example Microsoft makes AI services available through Azure, its PaaS service as Azure AI and Azure Cognitive Services; Google provides AIaaS through Google Cloud AI Solutions; and Amazon through AWS supplies a range of sector- and function- specific AI and ML services. This means that in any AI cloud deal, the normal range of contractual issues relating to intellectual property (for example IPR in training, testing and operational datasets, metadata and derived data; whether and if so how the CSP can use this data to inform its own datasets and models, etc; and IPR in computer-implemented inventions and computer–generated works) and AI ethics (principles, procedures and processes) needs also to be looked at through the lens of cloud service provision. This may be more

[30] For further information, see our white paper on '*Legal Aspects of Artificial Intelligence*' (September 2018) - http://www.kempitlaw.com/wp-content/uploads/2018/09/Legal-Aspects-of-AI-Kemp-IT-Law-v2.0-Sep-2018.pdf

complex where the CSP provides its AI and ML cloud services through generic terms and conditions and SLAs, etc., and where the applicable IPR clauses may not be immediately accessible (and may confer on the CSP broader rights than the customer is would like).

46. **Cloud services – distribution and indirect sales**. In the traditional 'as a licence' model, software is sold either directly from developer to customer through the software user licence or indirectly through intermediaries. If indirectly, the intermediary will normally act in one of three roles:

- in the ***buy/sell*** model the intermediary buys the right to resell the software (whether the customer receives its user licence from the developer direct or the intermediary). Here, the purchase and sale go through the reseller's P&L account as expense and revenue;
- in the ***agency*** model, the intermediary introduces the customer to the developer, who then sells the software direct to the customer through the software user licence and pays the intermediary a commission. Here, the commission only (and not the underlying sale) goes through the agent's P&L account as revenue; and
- in the ***fulfilment*** model, the intermediary fulfils the sale by the developer to the customer in return for payment of a service fee. Here again the fulfilment service fee only (and not the underlying sale) goes through the fulfilment service provider's P&L account as revenue.

As the cloud develops, the same business rationale for going indirect – focusing scarce resources in depth on the CSP's largest customers and achieving breadth by having the CSP's intermediaries address the market for smaller customers – will apply to selling cloud services as it applies to traditional software distribution. However, whereas the reseller is able to buy the right to the software user licence from the developer and sell it on to the end user, it is more challenging for the reseller to sell in the 'as a Service' model. This is because the customer wants to be assured of service provision (access to the software, SLAs, data protection and IS commitments, etc) and the reseller is generally not in a position to agree to and fulfil these commitments, other than on a back to back basis which would leave the customer without direct recourse to the CSP in the event of service failure.

For these reasons therefore 'distribution' of cloud services is developing not around the 'buy/sell' model but around the agency or fulfilment model, with the cloud services contract generally running directly between CSP and customer. The agency model can give rise to difficulties in jurisdictions whose laws may entitle the agent to an indemnity or other payment from the principal on termination of the relationship (like the Commercial Agents Directive in the EU)[31], so the fulfilment services model may merit consideration. In general terms, therefore the customer should normally consider contracting directly with the CSP and not the intermediary whatever the arrangements between the CSP and intermediary.

H. CONCLUSION

47. Conclusion. As IT's epic migration to the cloud gathers pace, cloud contracts are quickly moving centre stage for IT lawyers, and cloud contracting techniques in all areas of business are evolving rapidly. Data law (in the areas of data protection, security, sovereignty and data rights) is emerging as the key issue in cloud contracts,

[31] Council Directive 86/653/EEC of 18 December 1986 on the coordination of the laws of the Member States relating to self-employed commercial agents - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31986L0653&from=EN. The directive has been implemented into Member State's national laws.

closely followed by information security, software rights and service levels. As cloud techniques and services continue to proliferate, the combination of these technical innovations and the legal issues arising will see cloud computing law generally and cloud contracting more specifically continue to develop rapidly in the coming months and years.

Richard Kemp,
Kemp IT Law, London,
June 2019
richard.kemp@kempitlaw.com

KEMP IT LAW

IT Law at the Apex

Richard Kemp
Partner

T: 020 3011 1670
M: 07932 695 615
richard.kemp@kempitlaw.com