KEMP IT LAW

Tech Law at the Apex

White Paper

Demystifying Tech for Lawyers

Richard Kemp, January 2023

DEMYSTIFYING TECH
TABLE OF CONTENTS

TABLE OF FIGURES

KEMP IT LAW

Tech Law at the Apex

DEMYSTIFYING TECH[1]

A. AUDIENCE, PURPOSE AND SCOPE

1. **Who should read this white paper?** The primary audience for this white paper is the in-house lawyer who is not a Tech specialist and who works at an organisation that is not a Tech provider company, but which acquires IT. The secondary audience is the in-house lawyer at a Tech acquirer company looking after IT and related aspects of the business. The white paper may also be useful to the in-house lawyer at a Tech provider company on the sales side who wishes to understand what her or his counterpart at their Tech acquirer customer will be thinking about or looking out for.

2. **Purpose and scope**. This white paper provides an overview of the five main kinds of Tech and communications procurement and deployment: equipment, software, data, services and telecommunications (**Section B** below). IT also briefly examines the current trends in IT as they may affect the organisation (**Section C**).

   Previous editions of this white paper have considered the Tech lawyer's role in the organisation and Tech types and Tech trends together in a single white paper. In this edition, we have separated the Tech lawyer's role in the organisation into a stand-alone white paper which is also available on our website at www.kempitlaw.com.

   This white paper is intended as an introduction. It is not legal advice and is not intended to be comprehensive. In this white paper, we use 'IT' and 'Tech' interchangeably.

B. TYPES OF TECH/COMMUNICATIONS PROCUREMENT AND DEPLOYMENT

3. **Introduction**. To those unfamiliar with it, the range of Tech contracts and related legal matters may seem daunting. In demystifying, it is helpful to break the area down into its key component parts. These are, essentially, five:

   - equipment (**paragraph B.4**);
   - software (**B.5**);
   - data (**B.6**);
   - services (which we've divided into three:
     - development, outsourcing and support (**B.7**));
     - the cloud (**B.8**);
     - digital commerce (**B.9**)); and
   - telecoms (**B.10**).

4. **Equipment**. Equipment can be divided into two main types:

   a) ***User equipment*** covers PCs, laptops, tablets, smart phones, and other devices that the organisation's people use in their day-to-day work: in network terminology, "client-side".

[1] This is the fifth edition of our white paper on Demystifying Tech. It replaces the earlier editions: 4th – March 2021; 3rd – June 2018; 2nd – January 2017; and 1st – January 2016. This edition splits out Demystifying Tech and Demystifying Tech for Lawyers. Demystifying Tech for Lawyers is now a separate white paper available on our website at www.kempitlaw.com.

b) ***'Server-side' equipment*** historically consists of servers, storage devices, cabled and Wi-Fi networking, back-up power sources, routers, switches and the like. Other equipment also includes the organisation's telephones and communications equipment together with document production and other office equipment.

5. **Software**. Computer software (programs) is a set of instructions that tells the computer what to do. It can be categorised by ***type of code***, ***development model***, whether ***product*** or ***bespoke***, type of ***function***, ***licensing and distribution*** and ***delivery model***.

a) ***Code type***: a computer program is generally written as *source code*, a form in which it is human readable. For source code to be run on and understood by a computer it needs to be *compiled* (translated) into *machine code*, a version of the program in binary format (consisting of 0s and 1s) that is not human readable. Machine code is also known as *object*, *binary* or *machine-readable* code and the program in this form is known as an *executable*.

b) ***Development model***:

- software was traditionally developed in a highly structured ("***cathedral***") way and on a proprietary model by developers whose ownership of the copyright in the code is the asset they license and monetise. Proprietary developers typically just license the object code and are loath to license source code (except through a mechanism called *escrow* where the source code is deposited with a trusted third-party escrow agent authorised to release it to licensees on triggering events like the developer's insolvency).

- This model has been successfully challenged by open-source software ("***OSS***"), a community development model that is much less structured ("***bazaar***") and where the underlying source code is made freely available under standard licences. Marc Andreessen, the co-founder of web browser Netscape, famously said in 2011 that software was eating the world, and to that aphorism may be added that OSS is eating software.

- OSS has long since become ubiquitous and most organisations now operate in a mixed environment using both proprietary software and OSS. It's important to appreciate that the difference between proprietary software and OSS is not in the code (which is the same in both cases) but in the licensing 'wrapper' applied to the software.

- The key OSS risk to be aware of is that some OSS licences (like the General Public Licence ("**GPL**") and Lesser General Public Licence ("**LGPL**") of the Free Software Foundation ("**FSF**")) operate an 'inheritance' (or 'copyleft') requirement. This means that proprietary software interacting with this kind of OSS may in certain cases itself become compulsorily open sourced as a condition of using the OSS in the first place.

Recent years have seen a decline in the popularity of copyleft OSS licences and a corresponding rise in the uptake of permissive licences like the Apache 2.0 and MIT licences that do not impose inheritance requirements. A recent report[2] shows the top 10 OSS licences by share as follows:

	Permissive (non-copyleft)					Copyleft			Weak copyleft	
Licence:	Apache 2.0	MIT	BSD3	BSD2	BSD	GPLv3	GPLv2	LGPLv2.1	MS Public	Eclipse 1.0
Share:	34%	30%	6%	2%	1%	11%	10%	3%	2%	1%

c) ***Product or bespoke***: Software can be either ***product*** (*off-the-shelf*), ***bespoke*** (*customised* or *developed*) or a mix of the two. Increasingly, for enterprise (large organisation) and SME (small to

[2] MEND-The-Complete-Guide-for-Open-Source-Licenses-2022.pdf.

medium enterprise) customers, off-the-shelf software needs to be tailored (tuned or parameterised) 'out of the box' to make it suitable for use.

d) ***Functionality type***: software is either *operating system*, *application* or *middleware*.

- The *operating system* ("**OS**") is the computer's traffic cop. It controls how resources – input, processing, memory, storage and output – are used in the most efficient way;
- *Application software* is the software functionality you use on your device (like an Office document on your laptop or an app on your smartphone) or through the Cloud or a server-based network across the enterprise (like Oracle, SAP or other enterprise resource planning ("**ERP**") software). The application sits on top of the OS. It requests the OS to use the computer's resources to perform tasks that it does not have permission to execute directly. These requests are made through *system calls* or *application programming interfaces* ("**APIs**"). A system call is a specific service request made directly by the application to the OS. An API is a set of requirements or specification which the application must comply with in order to obtain a particular service from the OS.
- In ERP/enterprise applications and the Cloud, *middleware* sits between the application and the OS to provide database and further resources to support the application.

e) ***Licensing and distribution***: like a book, software is protected as a literary work by copyright and so is ***licensed***. A licence is permission to do something that the law could otherwise stop you doing. Software licences are typically on a *subscription* (periodical, e.g. monthly or annually) or a *perpetual* (one-off) basis. Product software, as software licences (whether subscription or perpetual), is ***distributed*** directly by the developer itself or indirectly through the developer's 'channel'.

- In *direct* software distribution, the software developer directly licenses the end user to use the software on the terms of an End User License Agreement ("**EULA**") or (increasingly in the cloud world) Terms of Service ("**TOS**").
    - In business to consumer ("**B2C**") direct software licensing, the end user typically accepts the EULA or TOS by clicking on a radio button on the developer's website (whether or not they pay a fee) and downloading or otherwise accessing the software to use.
    - In business to business ("**B2B**") direct licensing, the end user and developer may negotiate and sign the EULA or TOS (for higher value deals) although here the trend is increasingly for EULAs and TOS to be click wrap accepted as in B2C;
- In *indirect* software distribution, an intermediary is interposed between the developer and the end user. Intermediation applies to both subscription and perpetual software licensing and increasingly to Cloud services and may take many forms.
    - In agency, the agent intermediary introduces the end user to the developer and takes a commission on the sale, with the commission revenue only (and not the sale price) going into the agent's P&L as income.
    - In distribution the distributor or reseller intermediary buys from the developer and sells on to the end user, with the purchase and sales price going into the distributor's or reseller's P&L as an expense (on the purchase) and income (on the (re)sale). Here, the EULA may still run directly between the developer and the user, where the distributor buys and sells not the EULA itself but the right to the EULA. (From the end user's point of view it is paying the price to the distributor or reseller directly but getting the EULA from the developer). Alternatively, the distributor may buy in and sell on the EULA.

Distribution may be one tier (developer → reseller → end user) or two tiers (developer → distributor → reseller → end user).

Distributors take a number of forms, including:

- OEMs (original equipment manufacturers) who typically pre-load software on a device and sell the two together;
- VARs (value added resellers) who sell the software and also provide other services, typically professional services in the case of enterprise software;
- wholesalers who focus on volume and the efficiency of their systems; and
- Appstore providers who connect mobile users to the developer (see **C.17** below).

The development of the Cloud is tending to disintermediate software distribution so that increasingly developers license end users directly, although here also we are seeing a growing distribution channel for Cloud services.

f) ***Delivery model***. Software is delivered (or deployed) "as a licence" or "as a service" (for SaaS, PaaS and IaaS, see **B.8** below). If as a licence, the software generally (but not always) resides on-premise – in the organisation's server room or data centre. If as a service, the software generally sits in-cloud at the data centre of the organisation's cloud service provider.

6. **Data**. As first computers and then software have tended to become commoditised, organisations are increasingly looking for competitive advantage to the data that they buy in, use and generate. As data becomes more valuable, data law is a rapidly growing field at the moment, encompassing:

a) ***data security***: the mix of legal, technical, operational and governance controls that an organisation puts in place to ensure desired security outcomes for its data;

b) ***data rights***: intellectual property ("**IP**"), contract and other rights and obligations in relation to data. Data is increasingly licensed akin to software, and several industries (for example, financial market data) have developed around an ecosystem of contracts and licences regulating usage and risk;

c) ***data protection***: the legal rights and duties that arise in relation to personal data (also known, particularly in the United States, as personally identifiable information) (see **C.12** below);

d) ***data sovereignty***: when a person's right to deal as they wish with their own data may be overridden, typically through involuntary disclosure to, or access by, a third party like the police or security services; and

e) other ***data regulation*** for example relating to non-personal data or in particular industry sectors like healthcare, financial services and the public sector.

It's all about ***being data driven*** at the moment - using business intelligence, AI and analytics software to harness the vast tides of information generated by the internet and predict what your organisation's customers are going to do next. These are complex and challenging projects to bring in. They require substantial developments in organisations' data architecture and underlying business processes as well as a structured approach to information governance around data classification, risk assessment, strategy, policy and processes. In short, involvement of all stakeholders but close cooperation at the centre of the effort will be especially necessary between the Chief Information Officer's team and the General Counsel's team.

7. **Services (1): development, outsourcing and support**. An organisation may contract with a service provider for the supply of a wide range of software and other IT-related service, including ***software development***, ***outsourcing and related services*** and ***maintenance and support***.

a) ***Software development***: An organisation may contract with a service provider for the supply of a range of software-related services. These may be supplied separately or bundled up with the supply of software, for example under a Master Software and Services Agreement ("**MSSA**"). Software development/customisation services are typically supplied on an "agile", "DevOps", "low-code" or "waterfall" basis.

- *Agile* is characterised by short, frequent, iterative, incremental development cycles where detailed specification and output requirements are not set out at the start but evolve through the project life-cycle, with attention focused on "sprints", "scrums" and resource points. In agile, role delineation (product owner, development team, scrum master, stakeholders, etc), communication, governance and project management are all at a premium.
- *DevOps*: As development cycles speed up, software development, operations and support are becoming increasingly integrated and Agile itself is evolving into a form of continuous development and improvement known as DevOps.
- *Low-code*: Low-code development can reduce time to value still further by enabling application software to be created through a GUI (graphical user interface) by an extended range of stakeholders who may not have (or need) particular coding skills.
- *Waterfall*: By contrast, waterfall is the traditional development mode characterised by sequential phases: *specifying requirements* → *design* → *coding* → *testing* → *error correction* → *integration* → *acceptance* → *deployment* → *support and maintenance*. Here, emphasis is on the charging structure (T&M, for time and materials, or fixed price), specification, project or implementation plan and demonstrated acceptance.

Key points for this sort of services agreement (whether agile, DevOps, low-code or waterfall) include:

- transitioning/cutting-over from the old to the new system;
- integration / interoperability with existing and third-party systems;
- maintenance and support; and
- futureproofing – backwards / forwards compatibility with other software.

b) ***Outsourcing and related services***: outsourcing is traditionally characterised as the handing over to an external service provider of a previously internally delivered function or business process. Services outsourced are generally tech-based or enabled and include back office services like:

- desktop and other IT services;
- HR;
- finance;
- accounting;
- legal process;
- front office call centre; and
- other customer-related services.

It has been said that Cloud uptake and digital transformation mean that all businesses are software businesses, building or using applications, machine learning, advanced analytics and cloud services. Organisations must decide the 'make/buy' question – whether to 'make' (develop) or 'buy' (in) the desired requirement or service. When they 'buy', many of these requirements or services will be outsourced to third parties, so outsourcing itself is moving away from long term, monolithic deals to an environment with a number of cloud service and Tech providers supporting the organisation, each with more granular functions and services more closely integrated into the organisation's day to day operations.

The services agreement between the customer and provider sets out the terms on which the services will be provided. As in all project-type agreements, the customer will want the outsourced service to be delivered on time, on budget and to standard and it is against this background that the agreement will identify the key performance indicators ("**KPIs**") and service level agreement ("**SLA**") that the provider commits to. The customer's staff may in certain circumstances transfer to the provider and the *Transfer of Undertakings (Protection of Employment) Regulations 2006* (*SI/2006/246*) (TUPE) will be relevant in this situation.

Although outsourcing agreements have tended to shorten, there is still a need for the customer to consider issues around:

- audit (showing that the provider has kept to the contract terms);
- Tech refresh (showing that the provider has kept up with commercially available Tech);
- benchmarking (showing that the provider has kept competitive on pricing and occasionally other terms); and
- "most favoured nation" (showing that the provider has not given an equivalent customer a better deal on pricing or other terms).

It is important for the customer to put in place appropriate internal resources, roles, governance and other mechanisms to manage the provider's service during the contract lifecycle. The customer should also establish exit/disengagement arrangements if the service is taken back in house or transferred to another provider at the end of the contract.

c) ***Maintenance and support***: Typically maintenance is charged by reference to price of the kit or the fee for the software. Software maintenance costs typically work out at around 20% per annum of a perpetual licence fee but are wrapped up in the periodical fee in the case of a cloud or other subscription licence. Service is generally offered on a tiered basis depending on the level of support purchased (gold, silver, platinum, etc.,) and the seriousness of the fault (for example: tier 1 – system unusable; tier 2 – major outage, some functionality remaining; tier 3 – all other faults). Market practice is generally for the provider not to commit to fix each fault but to commit to respond within a certain time ("TTR" or time to respond) and to escalate unfixed faults up through the provider's organisation.

8. **Services (2): the cloud**. The classic NIST definition[3] of the cloud specifies a type of computing with five key characteristics, three service models and four deployment models.

a) ***Five characteristics***: the cloud characteristics are:

(i) *on demand self-service*;

(ii) *network/internet access*;

(iii) *one-to-many provisioning* (resource pooling or demand diversification);

(iv) *rapid scaling* (elasticity); and

(v) measured *(metered) service*.

[3] available at http://www.nist.gov/itl/cloud/

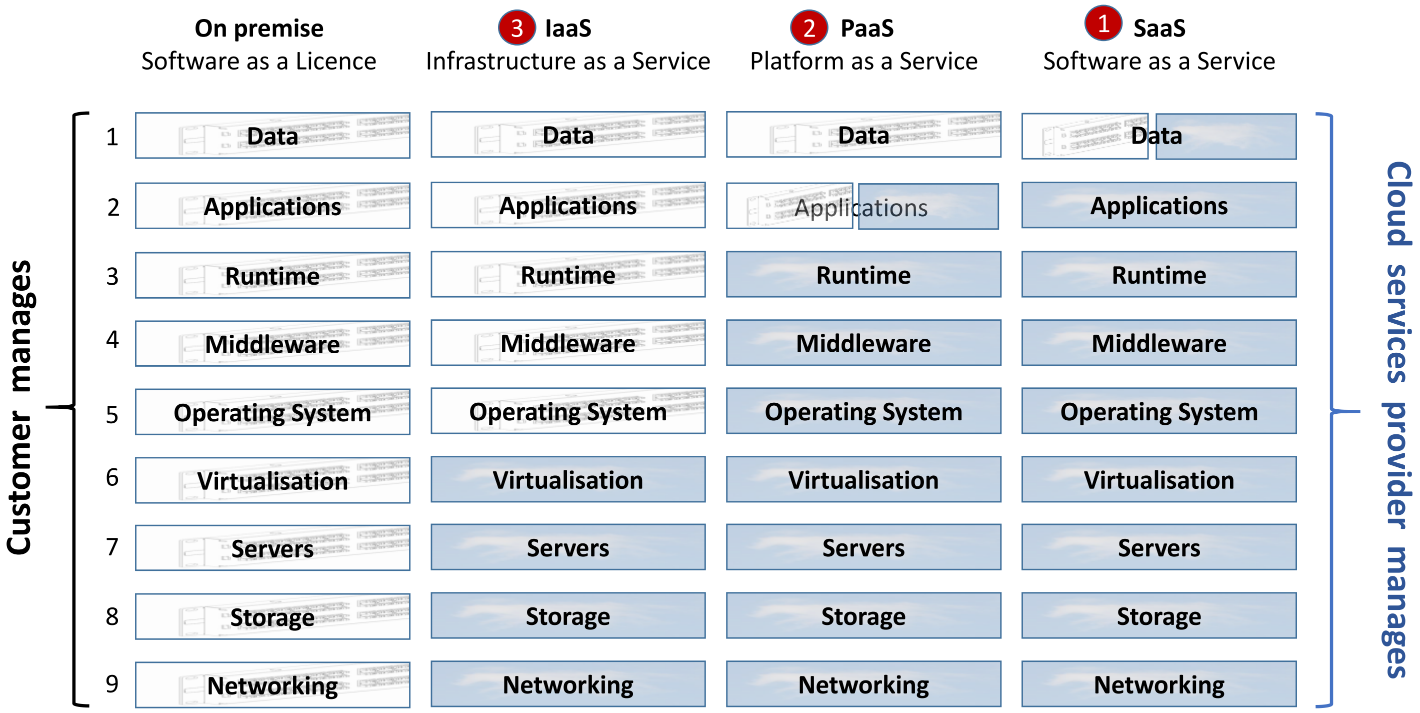
b) ***Three Service models***: the elements of the three cloud service models are shown at 1, 2 and 3 in Figure 1 below:

(i) *Software as a Service* (SaaS)*;*

(ii) *Platform as a Services* (PaaS); and

(iii) *Infrastructure as a Service (*IaaS*)*.

Figure 1: Software as a Licence to Software as a Service: the Cloud Service Model Continuum



	On premise Software as a Licence	3 **IaaS** Infrastructure as a Service	2 **PaaS** Platform as a Service	1 **SaaS** Software as a Service
1	**Data**	**Data**	**Data**	**Data**
2	**Applications**	**Applications**	Applications	**Applications**
3	**Runtime**	**Runtime**	**Runtime**	**Runtime**
4	**Middleware**	**Middleware**	**Middleware**	**Middleware**
5	**Operating System**	**Operating System**	**Operating System**	**Operating System**
6	**Virtualisation**	**Virtualisation**	**Virtualisation**	**Virtualisation**
7	**Servers**	**Servers**	**Servers**	**Servers**
8	**Storage**	**Storage**	**Storage**	**Storage**
9	**Networking**	**Networking**	**Networking**	**Networking**

c) ***Four deployment models***: these are:

(i) *private cloud* - where infrastructure, platform and/or software are used solely for a single Cloud Service Customer ("**CSC**");

(ii) *community cloud* - for use by a community of CSCs, rather than a single CSC;

(iii) *public cloud* – where service is provided to customers on a multi-tenant basis. (A useful analogy here is that the CSCs take rooms at the cloud provider's hotel); and

(iv) *hybrid cloud* - private cloud with access to public cloud to manage peaks.

As the cloud develops, it is increasingly common to speak of its 'core' and 'edge', and 'containers':

- the *core* is the cloud's engine room - the 1000 or so hyperscale, and all the 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 cost efficiencies, edge computing enables data generated by IoT and other devices to be processed close to source and away from the core;
- *containers* are small, discrete, independently deployable software applications designed to run anywhere and that carry the minimum resources to do a specific job. Containers boost the cloud's

efficiency by enabling routine processing tasks to be carried out on the edge where the data is generated, avoiding the unnecessary journey to the core and back again.

Hyper-scale cloud data centres are the engine room of digital transformation - think $1bn+ investments, 1m+ square foot data centres with 350,000+ servers using vast amounts of energy. The growth of cloud computing is driven by a number of factors, chief among which is price. At scale, the price premium of private over public cloud is around ten times. Cloud service revenues are growing prodigiously, causing the price of cloud services to decline, a key point for buyers to look out for.

Enterprise IT is midway through a major shift that is seeing the cloud's share of Tech move up to well over half. The cloud's development is startling: driven by the Internet of Things (IoT) and AI, data volumes created are growing strongly. Data created is currently two orders of magnitude (100x) higher than data stored, so data stored in the cloud's data centre 'core' has some catching up to do, and in 5 years' time will be 5x to 10x higher than today. At the same time, cloud power consumption rises 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 small fraction of what it is today even as data volumes stored rise exponentially.

The cloud provides users with a range of benefits and opportunities. These include:

- provisioning flexibility;
- access to new services;
- assisting digital transformation;
- speed of deployment; and
- cost efficiencies.

However, business operates in an environment that increasingly emphasises the criticality of cloud and data security. As computing workloads move to the cloud, the benefits of cloud provisioning need therefore to be weighed and balanced against security legal risks and obligations. The practical consequence of this is that organisations are establishing cloud security and compliance frameworks and governance to manage the range of cloud security duties and to assess and manage the risks involved.

9. **Services (3): digital commerce**. Digitisation is transforming how we live and work. As the cloud expands, services migrate online and new digital business patterns develop, a large and growing range of integrated, re-engineered and automated business-related services are emerging that are either completely new or were previously carried out with far greater human intervention. It may assist to understand the scope and range of digital commerce by categorising the services concerned as:

a) ***Online ordering of physical goods***: for example, delivery of tangible items through Amazon or food through Ocado;

b) ***Online ordering and delivery (fulfilment) of digital content protected by copyright***: for example, games, music, films, video, broadcasting or news. The Consumer Rights Act 2015 introduced digital content as a new separate category of supply alongside goods and services. As "data which are produced and supplied in digital form", digital content covers a wide range of digital products, but technically excludes the delivery mechanism for the content concerned.

c) ***Online ordering and delivery (fulfilment) of other digital services***: for example, tickets, digital subscriptions, and hotel reservations.

d) ***Communications services***: for example, mobile voice and data, broadband internet and broadcast.

e) ***Social media***: according to business data platform Statista, as of mid-2022, six platforms had more than a billion active users: Facebook, YouTube, WhatsApp, Instagram, WeChat, TikTok and Facebook Messenger; with a further six each between 500m and 700m: Douyin, QQ, Sina Weibo, Kuaishou, Snapchat and Telegram.

f) ***'XTech'***: where 'X' is a particular vertical undergoing digital transformation (e.g. AdTech, EdTech, FinTech, FoodTech, LawTech, MedTech and RetailTech).

The combination of the cloud and Fourth Industrial Revolution technologies like AI, blockchain, process automation and autonomous systems is disrupting many traditional industries and business patterns; and digital transformation is leading to the world of 'everything as a [digital] service'. Consumers may have little choice if they want to take the service since they have to click accept many pages of terms. Business customers may have a greater say, although the price of the service compared to the value that the service represents to the business may be out of kilter. The degree of liability that the provider is willing to accept in the event of a breach may be significantly less than the customer wishes to accept. This should be checked carefully in digital services contracts.

10. **Telecoms**. Telecoms services are typically provided on the basis of standard form agreements where there may as a practical matter be little opportunity to negotiate outside enterprise (large organisation) deals unless part of a larger agreement which is material to the telecoms provider. Telecoms contracts may be categorised by:

a) ***Type of network***: whether computer (ethernet, internet, wireless), telephone (public switched telephone network, or PSTN, packet switched network) radio, satellite, television broadcasting;

b) ***Type of transmission***: whether fixed line (for example, frame relay, ATM or multi-protocol label switching (MPLS)) or mobile (for example, 4G or 5G); and

c) ***Type of traffic***: voice, voice over IP (VoIP) data, video.

Communication service providers ("**CSPs**") are traditionally fixed telecommunications infrastructure operators (like incumbent telcos who trace their origins back to state-owned Postal Telegraph and Telephone organisations ("**PTTs**")) or mobile network operators ("**MNOs**") who provide mobile network connectivity, each under contract to their customers. MNOs may operate their own network of base stations and wireless links to the customer's handset or, as mobile virtual network operators ("**MVNOs**"), they may use another MNO's infrastructure and operate virtually. The distinction between fixed and mobile providers continues to erode.

Internet service providers ("**ISPs**") historically provide access or connection to the internet to their contract customers. ISPs can include CSPs and specialist providers. The development of the internet and (particularly) mobile apps has led to the development of over the top ("**OTT**") providers who supply their service "over the top" of, and without necessarily providing or billing their customers for, a network connection.

The terms CSP, ISP and OTT are becoming increasingly fluid as a provider organisation may have functions of each.

C. TECH TRENDS

11. **Introduction**. Tech is constantly changing and it is important to be aware of trends affecting how organisation's use it. It is also characterised by TLAs (three letter acronyms) and other jargon which can make even more inaccessible what are technically complex areas in the first place. With the principal aim of demystification, this section briefly considers as key current trends (but in no particular order) data protection (**paragraph C.12**), data and system security (**C.13**), Moore's law (**C.14**), digital transformation (**C.15**), virtualisation (**C.16**), the apps ecosystem (**C.17**), Web 3.0 (**C.18**), Industry 4.0 (**C.19**), the Internet of things (**C.20**), artificial intelligence (**C.21**), autonomous systems (**C.22**), blockchain and smart contracts (**C.23**), crypto (**C.24**), NFTS (**C.25**), property rights in digital assets (**C.25**), the Metaverse (**C.27**), quantum computing (**C.28**), sustainability in Tech (**C.29**) and Brexit and digital trade (**C.30**). All these trends influence organisations' use of Tech and they and the contracts and Tech legal work they represent are likely increasingly to come across the desk of the in-house lawyer.

12. **Data protection**. Data protection scarcely needs demystifying, but legal work in this area has settled back at a significantly higher level after than before May 2018 when the GDPR came into force. Data protection work volumes continue to grow as regulatory guidance expands and regulators start to flex their muscles on non-compliance. GDPR regulatory enforcement continues to gain traction and litigation and the continuing weaponization of data protection claims in the employment, B2B and international contexts grow apace.

    A potential curve ball to watch out for is the new ePrivacy Regulation (the source of the rules on cookies and cookie policies) that looks likely to extend the current ePrivacy Directive significantly and which is still going through the EU law making process.

    Particularly in cloud deals, the proportion of total page count attributable to data protection continues to increase, as providers' DPAs (data processing or protection addenda or agreements) become more complex and prescriptive. Negotiating DPAs can be time consuming, especially in the area of international transfers of personal data to outside the UK and EU, where the aftermath of the Schrems II decision in 2020 has increased complexity.

13. **Data and system security**. As business migrates online, and growth in big data, the cloud, social media and mobile accelerates, "trust" has emerged as the single biggest piece of grit in the wheels of growth. Cyber-attacks are growing in scale, sophistication and consequence, and the impact of each publicised incident is increased by media scrutiny.

    Getting data and system security right is therefore a critical objective for any organisation. Data and information system security (also known as cybersecurity) is a mix of management, legal, technical, operational and governance controls that an organisation puts in place to ensure desired security for its data and computer systems. It includes data protection (the legal rights and duties that arise specifically in relation to personal data) and data sovereignty (when a person's right to do as they wish with all their data may be overridden through involuntary disclosure to or access by a third party.

    In addition to data protection, more general cybsersecurity legislation is in force in the UK which stipulates minimum standards of security for certain classes of systems and operators. This includes the Network and Information Systems Regulations 2018 (SI 2018/506) ("**NIS Regulations**") which impose various cybersecurity and incident reporting obligations on two distinct classes of operator in the UK - certain ***digital service providers*** ("**RDSPs**") and ***operators of essential services*** in specific sectors that meet threshold operating requirements ("**OESs**"). Unlike data protection legislation, the

NIS Regulations focus on the security of network and information systems, rather than the security of personal data that the system processes. According to the Explanatory Memorandum to the NIS Regulations, the aim of this legislation is to:

> "establish a legal framework to ensure that essential services and selected digital service providers within the UK put in place adequate measures to improve the security of their network and information systems, with a particular focus on those services which if disrupted, could potentially cause significant damage to the UK's economy, society and individuals' welfare; and to ensure serious incidents are promptly reported to the competent authorities."

The EU has made increased cybersecurity a priority and has passed a revised version of the NIS Directive ("**NIS2**") and a Directive on the resilience of critical entities which toughen up standards and regulatory requirements. The new directives are to come into force in members states' national law by autumn 2024. The UK has consulted on changes to the NIS Regulations as part of its National Cyber Strategy to protect and promote the UK online.

14. **Moore's law**. In 1965, Gordon Moore, a co-founder of Intel, famously predicted that the number of transistors (microprocessors) on an integrated circuit (chip) would double approximately every two years. This empirical rule has held good for the last 60 years or so, meaning in practice is that computer processor speeds have doubled every 18 to 24 months. Although running out of steam as processor density starts to produce excess heat and other counter-productive side-effects, Moore's law is the fundamental driver that the computer industry has grown up with.

15. **Digital transformation**. Nebulous and potentially boundaryless, digital transformation can be challenging to articulate clearly. Diving in, we define it here as the investment in technologies, people and processes by an organisation to optimise its digital business capabilities. Even before the Covid-19 pandemic hit, digital transformation had emerged as the top priority in the organisation for technology initiatives, with (in roughly decreasing order):

- cloud as key digital transformation journey enabler;
- a much clearer focus on cybersecurity, data protection, compliance and governance;
- increasing investment in data analytics, AI and machine learning; and
- 'always on' software development through DevOps, low-code and Tech management as a service.

The Covid-19 pandemic accelerated these trends in a way unforeseeable before it struck, which can be seen by the growth in UK internet retail sales 2019 compared to the period before. At the macro level, the combination in 2020 and 2021 of strong internet growth, lockdown and the resulting hefty shove online is behind these figures, although the bursting of the Tech bubble and rising inflation, interest rates and energy costs in 2022 have brought the pace of the growth back to earth. These trends in the high street have stood as proxy to other sectors where digital transformation continues to accelerate (like travel, leisure, hospitality, healthcare and financial services) as well as to other walks of life (like legal and other professional services) where digital transformation is starting to make a real difference.

Digital transformation isn't occurring only in vertical sectors however. The cloud sets the scene for digital transformation whatever the sector, and horizontal areas that until very recently were the province of large numbers of human boots on the ground are now being cloudified and automated.

Nowhere is this more pronounced than in cybersecurity, where automating incident detection and response, privileged access management and data loss prevention are starting to remove some of the compliance and governance headaches, or at least enabling them to be managed in a more structured, proactive way.

16. **Virtualisation**. Virtualisation is the technique of using software to run more than one operating system on a host computer (***platform virtualisation***) or to reach computing resources that ordinary software cannot reach by aggregating individual computing resources into a smaller number of powerful resources (***resource virtualisation***). The ***hypervisor*** is the software that allows the creation or supervision of multiple virtual operating systems running simultaneously on the same computer – effectively creating multiple virtual platforms on one physical machine. As such, virtualisation and the hypervisor are integral parts of cloud computing as they allow service in large data centres to be used much more effectively and efficiently. Virtualisation is extending to the operating system (see 'containerisation' at **B.8** above).

17. **The apps ecosystem**. A mobile app is a small (in terms of lines of code) piece of application software that resides on a smartphone, tablet or other mobile device as a front end that enables the device user to access the app provider's service at the back end. The contractual ecosystem in this scenario can be quite complex and the actors in it are typically:

    a) The ***software developer*** of the app – typically the 'front end' (as the app itself resides on the user's device) – along with the 'back end' (the e- or digital commerce function that captures the order or provides the service). An app which is self-contained (e.g. a clock) will not have a back-end;

    b) The ***corporate vendor***, who could be a large or small service provider commercialising the mobile app as a way to fulfil sales – for example, a hotel chain selling hotel rooms; an online travel provider selling tickets; a digital content provider supplying news, film, TV, music, games, etc to their customers' mobiles; or a retailer or e-tailer (e-commerce retailer) wishing to develop its online distribution through a mobile app;

    c) The ***appstore provider*** who operates the systems or market-place where apps can be obtained and downloaded;

    d) A ***payment services provider*** who routes payments from the end user customer to the corporate vendor and may be a business unit of the appstore provider or a third party; and

    e) The ***end user customer*** of the app.

18. **Web 3.0**. A feature of the internet landscape currently is the rise of the distributed web, based on:

    - open-source frameworks for publishing lightweight, peer to peer applications;
    - decentralised data storage (like Holochain);
    - encrypted identity verification (like Keybase); and
    - third-party service integration (like Electron).

    The distributed web may herald a move away from the centralised platforms of web 2.0 and towards a more user-centric, "self-sovereign" internet. But this new web world – where there's no "canonical" single version of the truth as the data is stored on each user's device – may make the role of publishers and app developers more challenging in terms of intermediary liability, where the rules are set to tighten and effective notice and take down may no longer be in their gift. As ever, regulation struggles somewhat to keep up with the tech.

19. **Industry 4.0**. The fourth industrial revolution – after steam, electricity and computing – is the term that has been popularised by Mr Klaus Schwab, the founder of the Davos World Economic Forum, for the digital transformation that is now well under way. As digital innovation starts to transform our physical, digital and biological worlds, Mr Schwab's thesis is that we are in a time of vast ranges of Tech-driven change. The Internet of things, blockchain, AI, 3D manufacturing, virtual reality and a number of other areas overviewed in this note are areas of change that have already moved to the mainstream. Other areas, including autonomous vehicles, connected homes, neurotechnologies, robotics and smart cities are not far behind.

20. **The Internet of things**. As the cost of cameras and other sensors continues to decline, increasing numbers of things connect to the internet. Statistics provider Statista estimated there were 40 billion things connected to the internet in 2002, and that this will almost double to 75 billion by 2025 as the IoT develops in all its forms, from implantable technologies, the wearable internet and the connected home to autonomous vehicles and Smart Cities. That will amount to just around 10 IoT devices per person on average by 2025.

21. **Artificial Intelligence**. AI has moved definitively into the mainstream. It can be represented as the twinned convergences of social, data, data centres and mobile (on the one hand) and of machine processing, learning, perception and control (on the other).

    a) ***Machine processing***: This is fuelled by Moore's Law (see **C.14**).

    b) ***Machine learning***: Deep learning, a machine learning technique, is AI's "killer app" enabler. It works by first using large training datasets to teach AI software to accurately recognise patterns from images, sounds and other input data in what are called "artificial neural networks", so called because they consist of networks of simple information processing units known as "neurons" and take inspiration from the structure of the human brain. Once trained, the software's decreasing error rate enables it to make increasingly accurate predictions. Deep learning is the core technology behind the current rapid uptake of AI in a wide variety of business sectors from due diligence and e-discovery by law firms to the evolution of autonomous vehicles.

       Great strides are being made in the accuracy of predictive AI software powered by deep learning. Captioning AI software now creates captions that are more descriptive and accurate than captions for the same images written by humans. For some years now the accuracy of speech transcription AI software has met or exceeded that of human transcribers. This pattern (using the machine learning software to reduce prediction error through training and fine tuning, then letting the software loose on the workloads it is to process) is at the core of AI in professional services. It is behind the AI arms race in law (standardising componentry of due diligence, e-discovery, property title reports, regulatory compliance and contract management) accountancy (audit processes, tax compliance, risk) and insurance (coupled with IoT sensors), for example.

    c) ***Machine perception***: Machine learning techniques when combined with increasingly powerful and inexpensive cameras and other sensors are accelerating machine perception. Machine perception is the ability of processors to analyse data (whether as images, sound, text, unstructured data or any combination) and accurately recognise and describe people, objects and actions.

       - ***Computer vision*** is currently the most prominent form of machine perception, with applications including face, object and activity recognition and video labelling.
       - ***Speech recognition*** is another area where machine perception is developing quickly as the error rate has reduced substantially over the last few years.

- ***Natural language processing*** is becoming a primary human user interface for AI systems. Enabled by increasing accuracy in voice recognition, systems can respond to one-way user input requests and (as with ChatGPT) are starting to interact in two-way conversations.

d) ***Machine control*** is the design of robots and automated machines using better, lighter materials and improved control mechanisms to enhance the speed and sensitivity of machine response in 'sensing → planning → acting'. It adds to the combination of machine learning and machine perception in a static environment the ability to move in an interactive environment.

Essentially, mobile AI is more challenging than static AI and machine control builds on developments in machine learning (particularly reinforcement learning) and perception (particularly force and tactile perception and computer vision).

22. **Autonomous systems**. Autonomous vehicles continue to be in the headlines, but progress is being made also in autonomous modes of other types of transport – ships, trains and UAVs (drones and other unmanned aerial vehicles). The regulatory regimes, particularly around liability and insurance, will continue to develop at pace.

Areas of further development for autonomous systems include delivery and logistics (drones delivering your online orders are closer than you may think) and especially factories and warehouses.

23. **The blockchain and smart contracts**. The blockchain is a comprehensive, always up to date accounting record or ledger of who holds what or who transferred what to whom. The 'what' in the blockchain is virtually anything that can be recorded – physical assets like diamonds and land as well as intangibles like electronic cash, cryptocurrencies (se **C.24**), transactions in securities and other financial instruments, and records of government interaction with citizens.

There are two key features of the blockchain. First, it works through cryptography – authenticating parties' identities and creating immutable hashes (***digests***) of each ledger record, the current page of records (***block***) and the binding that links (***chains***) each block to the earlier ones. Second, instead of one person keeping one instance as 'single version of the truth', the blockchain ledger is distributed: a complete, current copy is held on the computers of each of the network participants (***miner***s) who help keep it up to date.

Significant hurdles to Blockchain in everyday use remain. First, given the breadth and area of potential applications, many regulatory issues need to be resolved. Second, blockchain is fragmented and the many different ecosystems need to agree common standards in order to all work together. Third, the blockchain is power hungry: greener and more efficient power usage will be key to bigger blockchains.

Overcoming these hurdles paves the way for 'smart contracts', software code representing a self-executing agreement as an arrangement that the computer can make, verify, execute and enforce automatically under conditions set in advance. The software can also be used to make and execute chains or bundles of contracts linked to each other, all operating autonomously and automatically. Smart contracts promise a range of benefits including lower costs, latency and error rates (through greater automation, less intermediation and less direct manual involvement) and are likely to enable new business and operating models.

Areas of potential use include:

- financial services: securities and financial instrument clearing and settlement, and insurance claim processing;
- healthcare: electronic patient records;
- media: royalty distribution; and

- public sector: government interaction with citizens, (registration, taxation and benefits).

24. **Cryptoassets**. Bitcoin, first released in 2009 as a 'peer to peer electronic cash system' is still the best-known blockchain application. It has led to the rapid development of cryptocurrencies as exchange mechanisms stored on the blockchain and using its encryption techniques to control issuance and funds transfer. Bitcoin, Ethereum, Ripple and Litecoin are among the most popular currencies. As they gain acceptance, the development of the financial services regulatory regime for cryptocurrencies is becoming increasingly important although recent insolvencies and instability in the sector has had an adverse impact on confidence in crypto.

25. **A property right in digital assets?** A notable UK development in 2022 was the Law Commission's consultation paper on Digital Assets, building on the 2019 Lawtech Delivery Panel's *Legal Statement on Cryptoassets and Smart Contracts*. The paper contains a powerful analysis of information and property rights and, in a low key but potentially far-reaching way, proposes a new kind of property for consultation.

    UK law traditionally recognises two types of personal property – 'things in possession' (goods and other tangible things) and 'things in action' (intangible things like debts, contract claims and intellectual property that ultimately you can only assert through legal action).

    The Law Commission proposes the 'data object' as a new, third type of personal property where it:

    - consists of data represented in an electronic medium;
    - exists 'there in the world', independently of any particular person and the legal system; and
    - is 'rivalrous' (i.e. its capacity for use is not unlimited – 'if I have it, you can't').

    The paper explores how these criteria might or might not apply to particular kinds of assets like digital files, email accounts, in-game digital assets, domain names, carbon emission schemes, crypto-tokens and NFTs. It then suggests how data objects could fit within existing legal concepts and principles as to creation, transfer of legal and equitable interests, security interests, custody, causes of action and remedies.

26. **NFTs**. NFTs have attracted much media attention, particularly in the art and luxury goods worlds, and the Law Commission paper devotes a chapter to them. The starting point is that, as an individually identifiable, cryptographically enabled token, an NFT can meet the criteria for a data object. It is in the link between that NFT and something else (for example, a digital drawing or image as a dataset external to the NFT's dataset) that challenging questions around permissioning, ownership and control can arise, especially where the NFT's contractual terms of use impact the legal rights in that something else.

    More technically from the legal perspective, there may well be property rights in both the internal dataset of the NFT and the external dataset that it links to; and whether, and if so how, the terms of use that apply to the NFT holder seek to confer rights or impose duties on the linked external dataset and its owner can then become critical.

27. **The Metaverse**. Advancing virtual, mixed and augmented realities herald the arrival of the metaverse, currently at the threshold of mainstream adoption in both the business and consumer spaces. A bit like the internet at the turn of the century, how the metaverse will develop is not yet clear. What is clear is that we are at a point where a range of AI-driven spatial technologies in the fields of location and context awareness, reality capture, design and visualisation and augmented, mixed and virtual reality are maturing at roughly the same time.

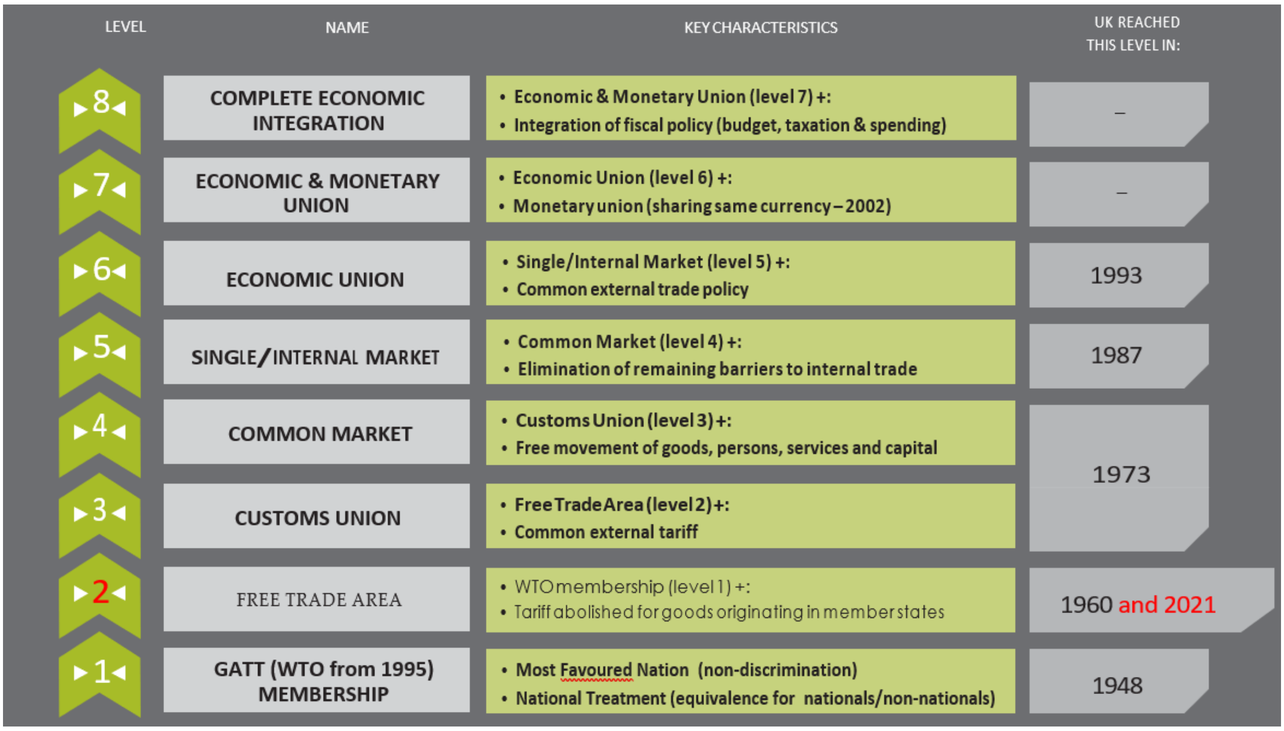
One possibility is that separate digital environments will build out as new infrastructure layers on top of the internet and coalesce around persistent (mass market) or temporary (smaller group) metaverses that leverage these technologies.

Potential examples here include film metaverses (driven by innovation in computer graphics and virtual production) and technical metaverses (driven by innovation in digital twinning as 3D models of physical world environments).

28. **Quantum computing**. Quantum computing is an idea whose time looks to be coming, even if it hasn't quite yet arrived. In digital computing, the basic unit of data processing is the bit (***b****inary dig****it***), which at any one time may have one of two values (0 or 1) or occupy one of two states (on or off). Quantum computing seeks to harness the subatomic physics of quantum mechanics where particles may occupy more than one value or state at the same time. This means that the qubit (***qu****antum computing's equivalent of the* ***b****inary dig****it***) can have more than one value or be in more than one state simultaneously. Quantum computing therefore has the potential to increase the number of computations that can be processed concurrently compared with digital computing, so enhancing computer speed just at the time when Moore's law may be running out of steam. Many large companies (including AT&T, Microsoft, Google, Hitachi and IBM) and specialists (including D-Wave, Rigetti and IonQ) are investing heavily in the field, although large scale adoption is still some way off.

29. **Sustainability in Tech.** Driven by climate awareness and geopolitical change, a growing theme in the Tech world at the moment and for the foreseeable future is sustainability – of each component in cloud and Tech infrastructure, in the mobiles, laptops and devices we use every day, and in the supply chains that put all this componentry together. As lawyers we will see these themes in new regulation, the adoption of technical standards in sustainable Tech and the policies and contractual terms that Tech organisations large and small require their suppliers to follow.

Figure 2: "Brexit means Brexit" means getting out at Level 2



LEVEL	NAME	KEY CHARACTERISTICS	UK REACHED THIS LEVEL IN:
8	COMPLETE ECONOMIC INTEGRATION	• Economic & Monetary Union (level 7) +: • Integration of fiscal policy (budget, taxation & spending)	–
7	ECONOMIC & MONETARY UNION	• Economic Union (level 6) +: • Monetary union (sharing same currency – 2002)	–
6	ECONOMIC UNION	• Single/Internal Market (level 5) +: • Common external trade policy	1993
5	SINGLE/INTERNAL MARKET	• Common Market (level 4) +: • Elimination of remaining barriers to internal trade	1987
4	COMMON MARKET	• Customs Union (level 3) +: • Free movement of goods, persons, services and capital	1973
3	CUSTOMS UNION	• Free Trade Area (level 2) +: • Common external tariff	
2	FREE TRADE AREA	• WTO membership (level 1) +: • Tariff abolished for goods originating in member states	1960 and 2021
1	GATT (WTO from 1995) MEMBERSHIP	• Most Favoured Nation (non-discrimination) • National Treatment (equivalence for nationals/non-nationals)	1948

30. **Brexit and digital trade**. Having ridden up six floors in the elevator of European economic integration since 1945 (see Figure 2 above), the UK finally got out at level 2, where it last was in 1960: tariff-free trade in UK- and EU- originating goods, bolted on to the WTO's basic principles of non-discrimination and equal treatment.

The EU/UK Trade and Cooperation Agreement (TCA) adds to this a number of high-level terms plus commitments to negotiate on services including seven pages aiming "to facilitate digital trade, to address unjustified barriers to trade enabled by electronic means and to ensure an open, secure and trustworthy online environment". The Government has called these out as "some of the most liberalising and modern digital trade provisions in the world", and "the first time the EU has agreed provisions on data in a free trade agreement".

The early 2020s were seminal years for digital regulation, as well pointing the direction that regulatory divergence between the UK and the EU will take.

As an example of the contortions that may lie ahead, many businesses are likely to end up with dual data protection compliance requirements, even with the adequacy decision for the UK (due anyway to expire on 27 June 2025), which will simplify the position compared with the alternative.

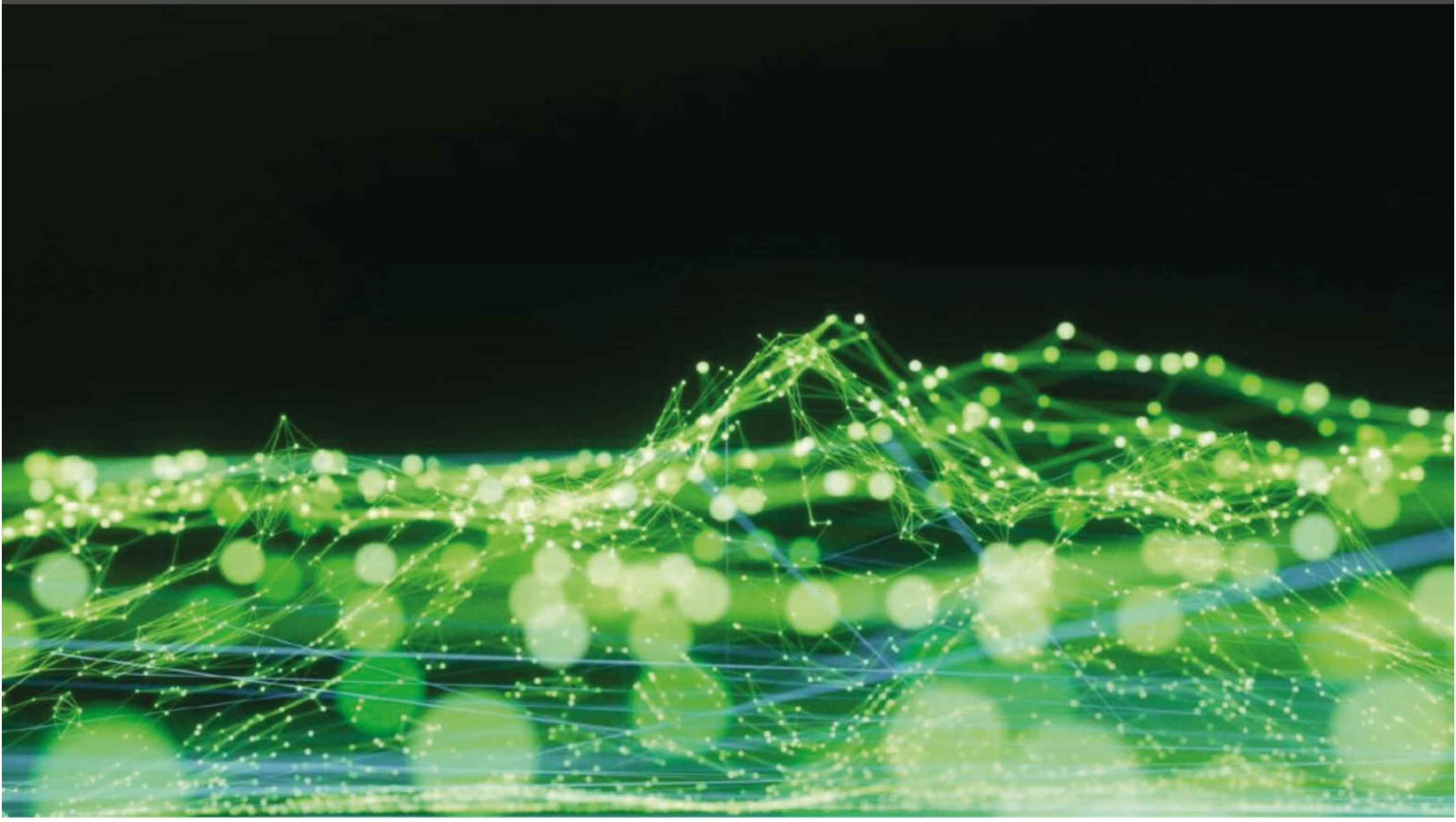
However, as well needing to comply with UK GDPR, a UK business will also be subject to EU GDPR if it offers goods or services to data subjects in the EU, monitors their behaviour or has an EU establishment. Whilst divergence is unlikely to be material early on, room for inconsistency and conflict between UK GDPR and EU GDPR will grow over time.

In the EU Withdrawal (Revocation and Reform) Bill 2022, the Government have proposed sunsetting at the end of 2023 all pre-Brexit EU law that has not been expressly continued in UK law by then. Many commentators have expressed alarm at the resources such a review would require, and at the time of writing (early 2023) it remains to be seen whether this policy will followed through. If it does, the bonfire of Brussels-based rules will add another layer of complexity to advising on UK Tech regulation.

Richard Kemp
Kemp IT Law LLP
London
January 2023

KEMP IT LAW

Tech Law at the Apex



Richard Kemp
Partner

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

Kemp IT Law LLP
www.kempitlaw.com

Registered office: 21 Napier Avenue, London SW6 3PS
Registered number: OC441771
Authorised and regulated by the SRA (No. 8000918)