ARTIFICIAL INTELLIGENCE | CLOUD COMPUTING | DATA LAW | DIGITAL COMMERCE | DIGITAL TRANSFORMATION | PRIVACY & SECURITY | SOFTWARE & SERVICES

KEMP IT LAW

IT Law at the Apex

White Paper

Demystifying Tech for non-Tech Lawyers (v4.0)

Richard Kemp

March 2021

DEMYSTIFYING TECH FOR NON-TECH LAWYERS
TABLE OF CONTENTS

TABLE OF FIGURES

DEMYSTIFYING TECH FOR NON-TECH LAWYERS[1]

A. AUDIENCE, PURPOSE AND SCOPE

1. **Who should read this practice note?** The primary audience for this practice note 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 note 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 or looking out for.

2. **Purpose and scope**. The purpose of this note is to provide an introduction to what to look out for in lawyering the organisation's procurement, deployment and governance of the Tech that it uses:

   - **Section B** overviews by way of introduction the five main kinds of tech and communications procurement and deployment: equipment, software, data, services and telecommunications.
   - **Section C** briefly looks at some of the current trends in Tech as they affect the organisation.
   - **Section D** considers the remit and role of the legal department and the Tech lawyer in lawyering the organisation's IT.
   - **Section E** to **H** provide practical pointers and tips in the areas of intellectual property rights (**E**), contracting for Tech (**F**), Tech regulation (**G**) and Tech governance (**H**).

   This practice note is an introduction. It is not legal advice and is not intended to be comprehensive.

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**) and 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".

   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***.

[1] This is the fourth edition of our note on Demystifying Tech for non-Tech Lawyers. It replaces the earlier editions: 3rd – June 2018; 2nd – January 2017; and 1st – January 2016.

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 organised ("*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 challenged by open-source software ("*OSS*"), a development model that is much less organised ("*bazaar*") and where the underlying source code is made freely available under standard licences.
- OSS has become mainstream 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) licences of the Free Software Foundation)) 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 MIT licence that do not impose inheritance requirements.

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 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 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 specification which the application must comply with in order to obtain a particular service from the OS.
- In ERP/enterprise applications, *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). In business to consumer (B2C) direct software licensing, the end user typically accepts the EULA by clicking on a radio button on the developer's website (whether or not they pay a fee) and downloading the software to use. In business to business (B2B) direct licensing, the end user and developer may sign the EULA (for higher value licences) although here the trend is increasingly for EULAs 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 may take many forms.
  - In agency, the agent 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 buys from the developer and sells to the end user, with the purchase and sales price going into the distributor's P&L as an expense (on the purchase) and income (on the (re)sale). Here, the EULA may 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 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 for professional or enterprise software; 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.

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) have become broader and deeper with the coming into force of the EU General Data Protection Regulation (*Regulation (EU) 2016/679*) (GDPR) (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.

It's all about ***being data driven*** at the moment - using business intelligence 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 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" 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.
- *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 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 and legal process and front office call centre and other customer-related services.

Cloud uptake and digital transformation have famously been said to mean that all businesses are software businesses, building and/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 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 often still a need for the customer to consider issues around audit (showing that the provider has kept to the contract terms), technology refresh (committing the provider to keep up with commercially available Tech), benchmarking (showing that the provider is keeping competitive on pricing and occasionally other terms) and "most favoured nation" (a commitment that the provider does not give a customer under an equivalent deal better 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 and also 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***: Maintenance and support are often neglected in practice. 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 fix on average within a certain time ("MTTF" or mean time to fix).

8. **Services (2): the cloud**. The classic NIST definition[2] 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*.

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

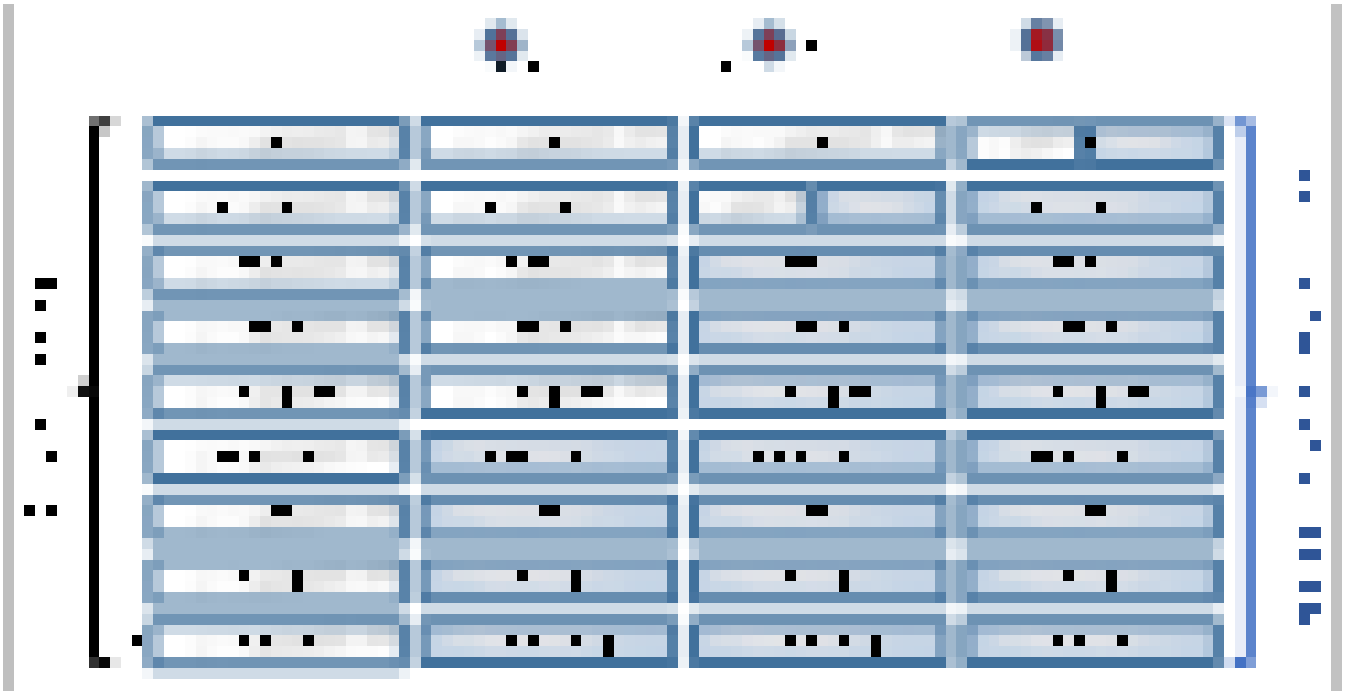
b) ***Three Service models***: the elements of the three cloud service models – (i) *SaaS*, (ii) *PaaS* and (iii) *IaaS* are shown at 1, 2 and 3 in Figure 1 below.

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 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.

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



Hyper-scale cloud data centres are the engine room of digital transformation - think $1bn+ investments, 1m+ square foot data centres with 250,000+ servers using enough energy to power a city. The growth of cloud computing is driven by a number of factors, chief among which is price. At scale, and after a large user has taken the first step away from on-premise to private cloud computing, 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 over half. The cloud's development is startling: driven by the Internet of Things (IoT), 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, which came into force on 1 October 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 end 2020, six platforms had more than a billion active users: Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram and WeChat, with a further six each between 500m and 700m: TikTok, QQ, Douyin, Sina Weibo, Telegram and Snapchat.

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

The combination of the cloud and Fourth Industrial Revolution technologies like AI, blockchain, process automation and autonomous devices 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, which are typically offered on standards terms by the provider.

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).

    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. 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**), blockchain and smart contracts (**C.22**), cryptocurrencies (**C.23**), quantum computing (**C.24**) and Brexit and digital trade (**C.25**). 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 data protection related legal work has settled back at a significantly higher level than before May 2018 when the GDPR came into force. GDPR regulatory enforcement is already gaining traction and we're starting to see an outbreak of

litigation and the continuing weaponization of data protection claims in the employment, B2B and international contexts.

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.

13. **Data and system security**. As business migrates online, and growth in big data, the cloud, social media and mobile accelerates, "trust" – a word that resonates in this context with both visceral and specific anxieties about your organisation's data in someone else's data centre – 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*** that operate in specific sectors and 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. The aim of this legislation is to implement minimum cybersecurity and transparency standards for those critical systems which could, if disrupted, potentially cause significant damage to the UK's economy, society and to individuals' welfare.

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 50 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 counter-productive side-effects like excess heat, Moore's law is the fundamental driver that the computer industry has grown up with.

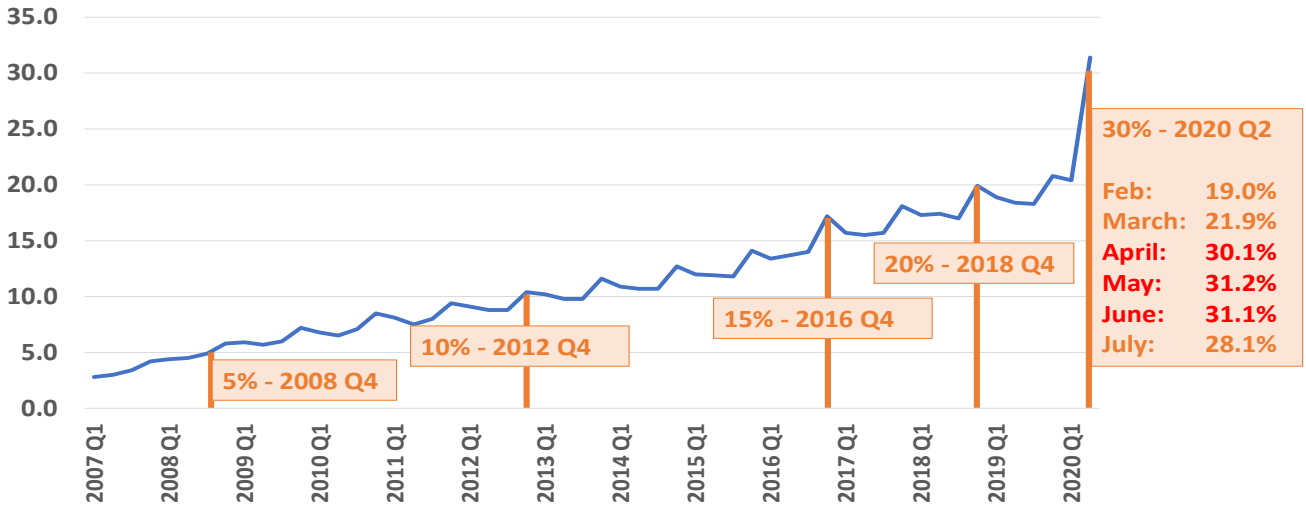
15. **Digital transformation**. Nebulous and potentially boundaryless, digital transformation can be challenging to articulate clearly. Diving in, we define it here as the investment in technologies, people and processes by an organisation to optimise its digital business capabilities. Even before the 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 and machine learning; and
    - 'always on' software development through DevOps and Tech management as a service.

    The pandemic has accelerated these trends in a way unforeseeable before it struck. How UK internet retail sales have grown illustrates this well (see Figure 2). Taking internet sales as a proportion of

total UK retail sales, it took four years for online sales to double from 5% to 10% (2008 to 2012), and another four to get to 15% (Q4 2016). But it then took only two years to reach 20% (Q4 2018) and, fuelled by the pandemic, just eighteen months to get from 20% to 30% (Q2 2020).

Figure 2: Internet sales as a percentage of total UK retail sales 2007-2020 (Source: ONS)



At the macro level, the combination of strong internet growth in 2018 and 2019, physical retail lockdown and a hefty shove online in 2020 is behind these figures. The acceleration of these trends in the high street stands as proxy to other sectors, whether the pandemic is a challenge (travel, leisure, hospitality) or an opportunity (healthcare, financial services), as well as to other walks of life, like legal services, where digital transformation is starting to make a real difference.

Digital transformation isn't occurring only in vertical sectors however. The cloud is a powerful digital transformation enabler, 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. 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 at the moment is the rise of the distributed web, based on open-source frameworks for publishing lightweight, peer to peer applications and 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. There are currently an estimated 12 billion connected things. This will rise to 31 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 under 4 IoT devices per person on average.

21. **Artificial Intelligence**. AI has moved into the mainstream. It can be represented as the twinned convergences of social, data, data centres and mobile and of machine processing, learning, perception and control (see Figure 3).

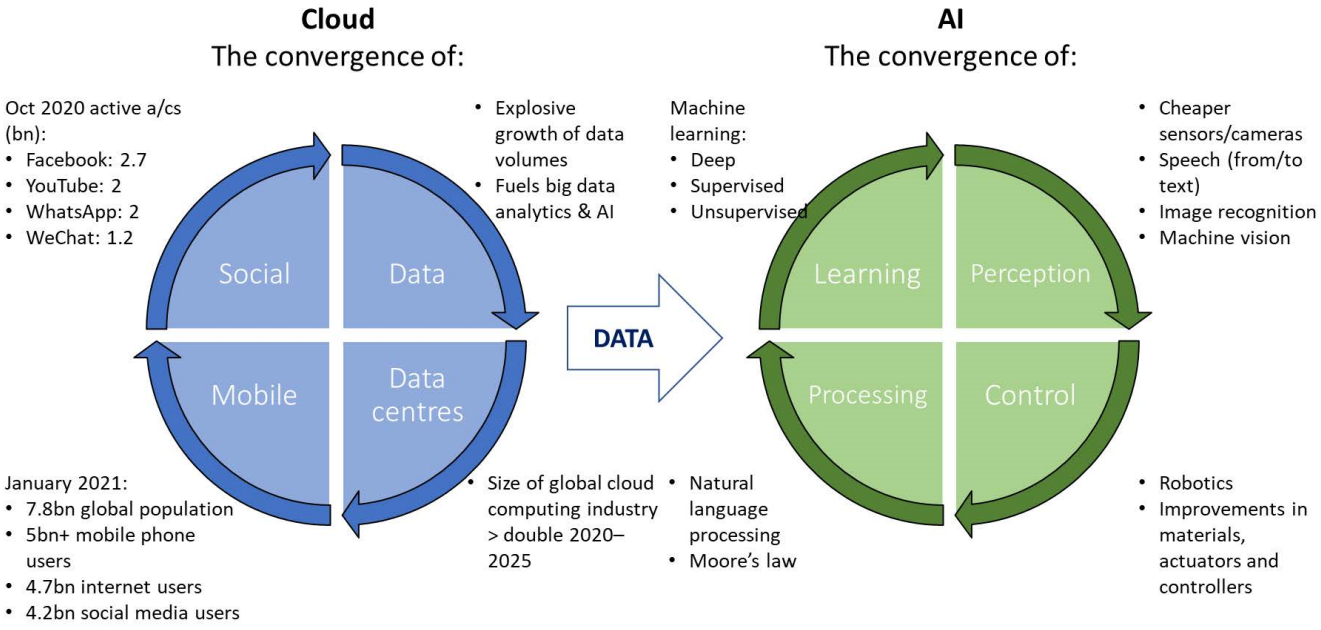
a) ***Machine processing***: This is fuelled by Moore's Law (see **C.14**).

b) ***Machine learning***: Deep learning, a machine learning technique, is emerging as 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. By late 2020 image captioning AI software was able to create captions that were 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 in litigation, property reports on title, regulatory compliance), accountancy (audit processes, tax compliance, risk) and (coupled with IoT sensors) insurance, for example.

Figure 3: Twinned convergences: the cloud and AI



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) to 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 emerging as 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 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. **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.23**), 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.

Blockchain is still in its infancy, and significant hurdles to commercial adoption 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 enormously power hungry 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 contract 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 securities and financial instrument clearing and settlement (financial services), insurance claim processing (financial services), electronic patient records (healthcare) and royalty distribution (music and media) and government interaction with citizens, (registration, taxation and benefits).

23. **Cryptocurrencies**. Bitcoin, first released in 2009 as a 'peer to peer electronic cash system' is the most well-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.

24. **Quantum computing**. Quantum computing is an idea whose time is coming, 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 may still be some way off.

25. **Brexit and digital trade**. So now we know what "Brexit means Brexit" means. Having ridden up six floors in the elevator of European economic integration since 1945 (see Figure 4 below), 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.

Figure 4: "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

The December 2020 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".

With significant legislation in the works in both Brussels and London, the early 2020s will be 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. During the transition period, the EU GDPR continued to apply in the UK pretty much as before and in February 2021 the EU announced that it would be

making an adequacy decision for the UK, 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.

D. LAWYERING THE ORGANISATION'S TECH

26. **Lawyering the organisation's Tech: Legal's remit and role**. Each organisation will approach how it lawyers its Tech functions and operations in a different way. For example, will all Tech contracts be reviewed by the Legal Department or only contracts above a certain threshold importance, whether established by price, duration or other criteria? Equally, to what extent will Legal be involved in Tech regulatory compliance and information and technology governance? Clarity on these issues will assist the legal group and the in-house Tech lawyer in carrying out their remit, role, responsibilities and authority levels.

27. **Working with other functions in the business**. In particular, the in-house Tech lawyer will need to understand remit, role, responsibilities and authority in her or his relationship with each of:

    a) the General Counsel;

    b) the Chief Information Officer and the IT Department

    c) the Procurement Group;

    d) the Chief Financial Officer and the Finance Department;

    e) the HR Department; and

    f) the Sales Department.

E. INTELLECTUAL PROPERTY RIGHTS

28. **Introduction**. The main IP rights in relation to Tech (principally software and data) are copyright (**paragraph E.29**), database right (**E.30**), confidentiality (**E.31**) and trade secrets (**E.32**) which are now briefly overviewed. Patents and rights to inventions can apply to software and business processes that manipulate and process data, although generally not in relation to data itself. Trademarks can apply to software, data and other Tech products.

29. **Copyright**. Copyright does what it says on the tine protects the form or expression of information but not the underlying information itself. It applies to software, certain databases, literary works, music, films, videos and broadcasts. It arises automatically by operation of law in the EU (so does not require to be registered). It is a formal remedy that does what it says on the tin and stops unauthorised copying (and the unauthorised carrying out of other acts protected by copyright, best seen as a 'bundle of rights' in this respect). A successful claim for copyright infringement will need to show:

    - that ***copyright subsists in the work*** – generally, that it is original (where the usual UK standard is low and normally that the work concerned has not been copied from elsewhere) and sufficient to warrant copyright protection (where the English courts typically take the pragmatic line that 'what is worth copying is worth protecting');
    - that the ***claimant owned*** or could otherwise sue on that copyright;

- that the ***work was within copyright*** (life plus seventy years in the case of software, databases and other literary works); and
- that the ***copyright had been infringed*** – for example, a qualitatively substantial part of the work had been reproduced without authorisation in circumstances where a copyright permitted act (fair dealing) exception did not apply.

30. **Database right.** Database right (a separate IP right from copyright) was introduced into English law in 1998, when the UK implemented the EU Database Directive. Database right arises in a database (essentially, a searchable collection of independent works) in whose 'obtaining, verifying or presentation' the maker has made a 'substantial investment'. The first owner of database right is generally the maker of the database as the person who takes the initiative in and assumes the risk of obtaining, verifying or presenting its contents. The right lasts for fifteen years from initial creation, effectively refreshed whenever 'any substantial change' is made. It is infringed by 'extraction and/or re-utilization' of a substantial part of the database contents on a one-off basis or repeatedly and systematically of insubstantial parts.

31. **Confidentiality**. Copyright and database right both protect expression and form rather than the substance of information. This means, somewhat counterintuitively, that equitable rules protecting confidentiality of information ('equity will intervene to enforce a confidence') very often provide the best form of IPR-type protection as they can protect the substance of data that is not generally publicly known. There is a long line of cases in the UK showing that protection can extend to aggregation of datasets even where parts of the data are in the public domain and so not otherwise confidential. Protection may also extend to second and subsequent generation data derived from the initial confidential data.

32. **Trade secrets**. The EU Trade Secrets Directive brings EU law more closely into line with Article 39 of the WTO TRIPS Agreement (which gives IPR protection to trade secrets as undisclosed information) and the US Uniform Trade Secrets Act. Article 2(1)(a) of the Directive sets out that a trade secret has three elements:

    a) ***secrecy*** in the sense that it is not as a body or in the precise configuration and assembly of its components generally known among those skilled in that subject;

    b) ***commercial value*** because it is secret; and

    c) reasonable steps must have been taken to ***keep it secret***.

    The Directive has been part of UK law since June 2018. As to the 'join' between the Directive and the UK law of confidence, the UK has confirmed that if UK law (of confidence) gives broader rights, a claimant can invoke them despite the Directive. In a legal environment where attaching IP rights to data, software and new technology more generally is challenging, trade secrecy is emerging as a likely candidate right, especially in a more digitally connected, AI- and cloud- enabled world.

F. TECH CONTRACTS

33. **Key tech contract types**. A material part of the in-house Tech lawyer's workload is likely to be negotiating and agreeing Tech contracts. These are of four main types – (i) contracts for equipment, (ii) licences of software and data, (iii) services agreements for software development, outsourcing and support, cloud services and digital commerce and (iv) telecoms services agreements. In many cases the supplier will be offering its standard terms to the Tech acquirer organisation where the in-house lawyer is working, so very often it will be a question of marking up and negotiating providers' form contracts.

34. **Equipment contracts**. Much equipment – whether computer devices of any description or network or office equipment – will be supplied on a commodity basis on standard terms, with a support contract as an extra. Equipment will either be purchased outright, rented or leased. Tax considerations will very often determine the type of contract chosen. In many cases equipment will be procured largely on cost grounds where scope for negotiation is likely to be limited. The working life of this sort of equipment is likely to be between two and five years so what happens during and at the end of the contract (trade in, upgrade, etc) needs to be considered at the outset.

35. **Software and data licences**. As software and services start increasingly to conflate through the move to the cloud, the "services" component of Tech contracts become more important. However, for software and data licences a range of terms needs to be considered including:

    a) scope of licence – making sure user can do everything it wants to do software or data;

    b) whether the user can develop its own software or derive or create new data from what has been originally licensed and in if so who owns it;

    c) the usual technical legal considerations around warranty and conformance to specification; security of licence and indemnity for intellectual property infringement claims from third parties; and liability limitations.

36. **Services agreements**. For most types of services contracts (and many of these points apply generally in the Tech contract area), the customer should consider:

    a) the range of ***pre-contract issues*** including:

        - supplier due diligence;
        - supplier stability;
        - customer service/dependence (what's the worst that can happen and how quickly can a replacement be obtained?).

        Much of this work will be undertaken by the procurement group, with whom the in-house lawyer will need to liaise closely;

    b) the range of ***lifecycle issues*** including:

        - *pricing*: in a longer term deal, make sure if market prices are going down that you are not 'beached' with higher prices. Consider benchmarking in larger deals (although cumbersome to implement) and open book pricing in appropriate cases
        - *performance*: KPIs, SLAs and service credit regime. The customer will want any service credit regime not to be the exclusive remedy for performance below contractual expectations. The provider will generally want the converse;
        - *availability*: particularly now mission critical services are starting to be entrusted to the cloud.
            - When is the service contracted to be made available?
            - What are the customer's responsibilities generally and what is the consequence of not performing them (relief event for provider, breach of contract by customer)?
            - If the service is being delivered via the Internet, it can be subject to its vagaries – how is this to be managed?
            - Is the provider dependent on any sub-contractors and if so, how is that to be managed?
        - *data*:

- How/when can I have it back?
- What are the supplier's commitments on return of customer data both during and after the contract?
- In what form will data be returned?
- How long is it from customer request to return?
- Will the customer be able to use the data in the form in which it is returned?
- Will the supplier "play nice" and return the data on termination whatever the reason for termination?

- *management of change*: customer requirements invariably change and the contract needs to be flexible enough to deal with this. Note that change control is where the supplier in a larger contract can claw back some of the control that it has lost in a competitive tender, so the customer needs to be aware to operate the change control mechanism and documentation effectively to counter this;
- *business continuity/disaster recovery*: the customer may get an enhanced backup service if it is prepared to pay higher fees. Don't forget to test at least annually the resilience of the backup and data return arrangements put in place under the agreement;
- *exit*: think about exit before you sign up and prepare a workable exit/ disengagement plan;

c) more ***technical legal issues*** including:

- making sure that the customer has full, unrestricted right and title to *intellectual property* in customer data and that the supplier is appropriately bound by confidentiality and non—disclosure obligations.
- on *liability*, market practice tends to be (but of course is not invariably) that:
  - both sides exclude consequential loss;
  - both sides limit direct loss by reference to the contract value or annual fees paid. Remember that under general contract law principles, direct loss - effectively, wasted expenditure (rewind to start) or the market costs of a replacement (wind on to the end) - tends to self-limit at a multiple less than two of the contract value.
  - on top of these points, the customer may look for unlimited liability and/or indemnity cover from the supplier for (i) IP infringement and breach of (ii) confidence, (iii) GDPR and (iv) security obligations although the supplier will want to limit its exposure here;
  - the supplier will want liability for non-payment not to count towards any cap.
  - both sides will not be able to exclude liability for the usual things (death or personal injury caused by negligence, fraud or fraudulent misrepresentation and breach of certain implied terms as the title, etc);
  - regulatory liability and liability for data loss or breach tend to be more heavily negotiated in larger services deals.

37. **Digital transformation lawyering 'do's' and 'don'ts'**. As digital transformation projects take up more of an organisation's resources and time, it's all about clarity, scope definition, relationships and objectives. From our seat deep inside the fourth industrial revolution, the range and speed of adoption of new IT techniques rippling out across business can appear daunting – Web 3.0, 4th Industrial Revolution, 5G, AI, blockchain, cloud, DevOps, IOT, mixed reality and Smart APIs to name but a few. But getting to clarity around what the tech does is an essential first step towards being able to scope it out and apply legal principles to it: clarity of legal analysis based on genuine understanding of the tech is a prerequisite for the team effort.

Along with understanding the tech goes the legal team's stakeholder role in helping shape the organisation's strategy, policies and processes around digital transformation, particularly in the areas of designing in compliance (privacy and data protection, cybersecurity, sector specific regulation), end to end data governance and DevOps' 'always on', shortened software life cycle. Writing up the foundational documents – from the vision, through the policy to the detailed processes – clearly and concisely and communicating them effectively enhances buy-in across the organisation.

38. **Digital transformation deal 'do's' and 'don'ts'**. The legal team's role in digital transformation compliance and deals gives it an enabling role in managing Digital transformation projects – whether strategic or tactical deals or strategic compliance – and in setting agendas and objectives.

    On the deals front, cloud due diligence, procurement and contracting are now in the mainstream, but as we move to 'everything as a service' (XaaS), understanding the basics of the different cloud service models (SaaS, PaaS and IaaS) and delivery models (public – a room at your hotel; private – my own room; and hybrid - combination) remains the first step (see Figure 1).

39. **Effective contract management is critical in digital transformation projects**. As the business models and contracting approaches of the major SaaS players mature, it's becoming increasingly common on a single larger digital transformation project to deal with the core SaaS provider, the professional services implementation partner and one or more providers of contiguous services. How the customer defines, scope and shapes the contract structure is critical. It may be impractical to get all parties involved to sign up to one contract, but in a series of bilateral contracts, aligning the dependencies between different providers puts a premium on effective contract management. Establishing from the outset a common approach to governance, project methodology, reporting standards, testing and structuring relief events can make all the difference here. In passing, AI as a Service (AIaaS) deals are becoming increasingly popular and aligning the customer's and the provider's ethics and data policies can be a challenge.

40. **A coherent and consistent approach to data is key**. A coherent and consistent approach to data in digital transformation deals is also key. We're not just talking about data protection and cybersecurity compliance – key though they are – but also a more standardised approach to data governance that looks at data both as corporate asset and as a source of potential risk or liability.

41. **DevOps**. As software development moves centre stage, with many organisations using their own apps and APIs in enhancing the customer experience, we're moving away from the sequential waterfall model, past Agile and towards DevOps, combining shorter development cycles (Dev) with continuous operational (Ops) delivery. In this world, effective internal policies around the following are key:
    - *software asset management*: ensuring proprietary software is used within licence scope;
    - *open source software*: managing residual risk around copyleft and OSS deployment; and
    - *source code management*: source code repository like GitHub.

42. **Growing importance of lawyering digital transformation**. Lawyering DT is becoming a core part of the organisation's skillset in successfully responding to the great shove online, and lawyers' unique combination of skills – getting to grips with the technology, applying evolving legal principles to how it's contracted for and used, formulating strategy and policy, helping assess risk, communication and relationship building – will continue to play an important role in ensuring that success.

G. TECH REGULATION

43. **Key regulatory areas**. The in-house lawyer looking after the organisation's IT is likely to have responsibility for the growing area where regulation and Tech intersect. Clearly, this may include many areas of business regulation and the following paragraphs call out data protection, data security and sector specific regulation.

44. **Data protection**. The in-house Tech lawyer may have responsibility as the organisation's data protection officer. Areas of concern include:

    a) establishing the lawful processing basis of all personal data it processes;

    b) the organisation's internal and external privacy and data protection policies;

    c) demonstrating compliance through records of processing, impact assessments, and privacy by design/default;

    d) operation of procedures and mechanisms for data subject rights;

    e) processes and procedures for management of data breaches and, in particular, whether or not to notify an event to the ICO;

    f) appropriate treatment of data protection and data sharing in the organisation's national and international contracts;

    g) overseas transfers; and

    h) anonymisation.

45. **Data security**. Organisations are increasingly focusing on a structured approach to the security of their data and this tends to consist of a mix management, legal, technical, operational and governments controls. The in-house IT lawyer is likely to find her or himself on the project team looking at data security and then dealing with implementation and management.

    Cyber attacks are growing in scale, sophistication and consequences, and the impact of each publicised incident is increased by media scrutiny. The NCSC (the National Cyber Security Centre, part of the UK's GCHQ) reports on cyber threats to business and notes at the moment as among major incident trends ransomware, DDoS attacks (distributed denial of service – bombarding and overloading systems so they fail), massive data breaches and supply chain infiltration with other significant incidents including CEO/senior executive business executive compromise (BEC) (email scams requesting urgent funds transfers) and cyber crime 'as a service'.

    Security is one of a number of rapidly developing areas of Tech law and regulation. These areas overlap to an extent and may best be thought of as providing different perspectives and frameworks from which to analyse and assess IT law issues.

46. **Regulation in your sector**. In addition to generic regulation, if the organisation operates in an area like financial, healthcare, travel or legal services or utilities, it will be subject to its own sector's regulatory regime. As Tech increasingly becomes the beating heart of business, sector specific regulation tends to apply more closely to the organisation's Tech operations. Special regimes may apply for outsourcing, the cloud, other critical IT, regulatory audit and reports, and treatment of data or IS breaches, etc., and these are likely to be within the remit of the in-house Tech lawyer

H. INFORMATION AND TECHNOLGY GOVERNANCE

47. **Governance**. Along with Tech contracts and Tech regulation, governance of the organisation's intellectual property assets, IT security, data and related operations is likely to be a key part of the in-house Tech lawyer's role. Here, the emphasis is on a structured approach enabling the organisation to gain maximum advantage in a secure, legally compliant way that balances rights and duties. In general terms, a structured approach will normally involve at least three elements. First, a strategy statement articulating the organisation's rationale, goals and governance arrangements. Second, a policy statement that fleshes out the high-level strategy statement and sets out how the governance will be implemented. Third, more detailed day-to-day processes and procedures for governance operation.

48. **Policies**. Tech-related areas where the organisation is likely to have been considering specific policies include the following:

    a) IT usage;

    b) Privacy/data protection/fair processing;

    c) Data security;

    d) 'Bring your own device';

    e) Monitoring at work;

    f) Homeworking; and

    g) Social media.

    The number of IT-related policies Tech buyer organisations are scheduling to their procurement contracts that the provider must comply with has grown sharply over the last few years, particularly in regulated businesses. Specific policies may include the following:

    i) Archiving and records retention;

    ii) Business continuity/disaster recovery management;

    iii) Code of business conduct and ethics for IT Vendors;

    iv) Data centre physical security;

    v) Electronic communications policy;

    vi) Information security policies – network, architecture and vendors

    vii) Sanitisation of electronic media for secure disposal

    viii) Sustainability principles

49. **Insurance**. Finally it is worth considering insurance arrangements in relation to risk management for the company's operations as regards IT. If the organisation operates a register of significant risks, consideration should be given how Tech governance and related matters are dealt with on the risk register.

KEMP IT LAW

IT Law at the Apex

Richard Kemp
Partner

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