KEMP IT LAW

Tech Law at the Apex

White Paper

Demystifying Tech Lawyering

Richard Kemp, January 2023

DEMYSTIFYING TECH LAWYERING

TABLE OF CONTENTS

DEMYSTIFYING TECH LAWYERING[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 an IT specialist and who works at an organisation that is not an IT provider company, but which acquires IT. The secondary audience is the in-house lawyer at an IT acquirer company looking after IT and related aspects of the business. The note may also be useful to the in-house lawyer at an IT provider company on the sales side who wishes to understand what her or his counterpart at their IT acquirer customer will be thinking about or looking out for.

2. **Purpose and scope**. This white paper provides an introduction to what to look out for in lawyering the organisation's Tech procurement, deployment and governance:

   - **Section B** considers the remit and role of the legal department and the IT lawyer in lawyering the organisation's IT.
   - **Sections C** to **F** provide practical pointers and tips in the areas of intellectual property rights (**C**), IT contracting (**D**), IT regulation (**E**) and IT governance (**F**).

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

   This practice note is 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. LAWYERING THE ORGANISATION'S IT

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

4. **Working with other functions in the business**. In particular, the in-house IT 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.

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

C. INTELLECTUAL PROPERTY RIGHTS

5. **Introduction**. The main IP rights in relation to IT (principally software and data) are copyright (**C.6**), database right (**C.7**), confidentiality (**C.8**) and trade secrets (**C.9**), 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 IT products. Patents and trademarks are not considered further here.

6. **Copyright**. Copyright 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 and therefore does not need to be registered. It is a formal remedy and 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 the work is original (where the usual UK standard is low and normally that the work has not been copied from elsewhere) and sufficient to warrant copyright protection (where the English courts traditionally take the pragmatic line that 'what is worth copying is worth protecting');
   - the claimant owned or could otherwise sue on that copyright;
   - the work was within copyright (life plus70 years in the case of software, databases and other literary works); and
   - 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 exception did not apply.

7. **Database right.** Database right (a separate IP right from copyright) was introduced into English law by the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032), which implemented the Database Directive (96/9/EC). 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 wherever 'any substantial change' is made. It is infringed by 'extraction and/or re-utilization' of a substantial part of the database contents whether on a one-off basis or repeatedly and systematically of otherwise insubstantial parts.

   Under the UK-EU withdrawal agreement, database right that subsisted in the UK or EEA before the end of the Brexit transition period (whether held by UK or EEA persons or businesses) continues to subsist in the UK and EEA for the rest of its duration. However, UK citizens, residents and businesses will no longer be eligible to receive or hold new EU database right after the end of the transition period. The government has legislated to create a new UK database right which may arise in databases created after the end of the transition period. It has done this by amending the Copyright and Rights in Databases Regulations 1997 to make them refer to the UK rather than to the EEA .The new right gives the same rights in the UK as the EU database right gives in the EEA, and for the same duration.

8. **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.

9. **Trade secrets**. The EU Trade Secrets Directive (Directive 2016/943/EU) brought 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 EU Trade Secrets Directive sets out that a trade secret has three elements:

   - it is *secret* - 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;
   - it has *commercial value* because it is secret; and
   - it is *kept secret* - reasonable steps must have been taken to keep it secret.

   The EU Trade Secrets 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.

D. TECH CONTRACTS

10. **Key Tech contract types**. A large part of the in-house Tech lawyer's workload is likely to be negotiating and agreeing Tech contracts. There are four main types of Tech contract:

    - contracts for equipment;
    - licences of software and data;
    - services agreement - for the cloud; software development, outsourcing and maintenance and support; and digital services; and
    - telecoms.

    In many cases the supplier will be offering its standard terms to the IT 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.

11. **Equipment contracts**. Most equipment (whether computers 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.

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

a) scope of licence – making sure the user can do everything it wants to do with the 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 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.

13. **Services agreements**. The customer will need to consider the following points:

a) a 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*: this is particularly important now mission critical services are widely 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 (for example, relief event for provider, breach of contract by the 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 subcontractors 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 return the data on termination whatever the reason for termination?

- *change management*: customer requirements invariably change and the contract needs to be flexible enough to deal with this. 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. The customer will need to understand how to operate the change control mechanism and documents 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 this before you sign the contract and prepare a workable exit or disengagement plan;

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

- ensuring 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.
- the scope of the supplier's *performance warranty* (for example, whether conformance with specification or re-performance of non-compliant services) and warranty and indemnity protection against third party IP rights infringement should be checked carefully.
- on *liability*, market practice tends to be that:
  - both sides exclude consequential loss;
  - both sides limit direct loss by reference to the contract value or annual fees paid or payable (or a multiple of them). 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.
  - the customer may look for unlimited liability and indemnity cover from the supplier for (i) IP infringement and breach of confidence/trade secrets, (ii) data protection and information security regulatory and contractual breach although the supplier will likely want to limit its exposure here.
  - the supplier will reasonably 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 information security and data loss or breach tend to be more heavily negotiated in larger services deals.

14. **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.

    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/ML, blockchain, Cloud, crypto, DevOps and low-

code, digital assets, IOT, the Metaverse and mixed reality, NFTs, Smart APIs and smart contracts, 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/low-code's '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.

15. **Digital transformation deal 'do's' and 'don'ts'**. The legal team's role in digital transformation compliance and digital transformation 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 DT 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.

16. **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 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.

17. **A coherent and consistent approach to data is key**. A coherent and consistent approach to data in DT 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.

18. **DevOps and low code**. 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 structured, sequential waterfall model, past Agile and towards DevOps and low-code, combining shorter development cycles (Dev) with continuous operational (Ops) delivery and where formal coding skills are not so necessary (low-code). In this world, effective internal policies around the following are key:

    - *software asset management*: ensuring proprietary third party software is used within licence scope and avoiding over-deployment;
    - *open source software ('**OSS**')*: managing residual risk around copyleft and OSS deployment; and
    - *source code management*: source code repository like GitHub.

19. **Growing importance of lawyering digital transformation**. Lawyering digital transformation 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.

E. IT REGULATION

20. **Key regulatory areas**. The in-house lawyer that looks after the organisation's IT is likely to have responsibility for the growing area where Tech and regulation intersect, which may include many areas of business regulation.

21. **Regulatory response to new IT techniques** . The development of new IT techniques (such as AI/ML, blockchain, Cloud, crypto, digital assets, IOT, the Metaverse, Smart APIs and smart contracts) has drawn a full-on regulatory response, most notably in the EU's comprehensive Digital Strategy and Policy Programme. Remarkably, at the time of writing (early 2023) over a dozen major new sets of rules are proposed, in transition or in force. Covering AI, cybersecurity, data, platforms, ePrivacy and healthcare and workforce data and product liability (see the table below), this extended toolbox of new rules represents the most complete and vigorous policy response to the demands of technology change yet seen anywhere.

Area / Measure	Content	Instrument* & status (winter '22)
Artificial Intelligence		
• AI Act	sets out harmonised rules on AI	Regulation, proposal of 21.04.21
Cybersecurity		
• Cyber Resilience Act	connected device software vulnerabilities	Regulation, proposal of 15.09.22
• Cyber Security Act	strengthens EU cybersecurity	Regulation of 17.04.19,
• NIS2 Directive	upgrades network and information systems directive	Directive of 14.12.22
• Critical Entities Resilience Directive	reduce vulnerabilities of critical entities	Directive of 14.12.22
Data		
• Data Act	harmonises rules on data fair access and use	Regulation, proposal of 23.02.22
• Data Governance Act	aims to ensure trust in data sharing, neutrality of data markets and public sector data use	Regulation in force on 24.06.22, most terms apply from 24.09.23
Online platforms		
• Digital Markets Act	aims to foster 'Big Tech' fair competition	Regulation in force on 01.11.22, most terms apply from April 2023
• Digital Services Act	regulates online services and intermediary service providers	Regulation in force on 18.11.22, most terms apply from Feb. 2024
Privacy and data protection		
• ePrivacy Regulation	replaces and overhauls Privacy and eCommunications Directive (2002/58)	Regulation, draft awaits European Parliament reading position

Area / Measure	Content	Instrument* & status (winter '22)
• Health Data Space Regulation	establishes a common space for individuals to manage, and entities to access, health, healthcare and genomic data. (First of several domain-specific common EU data spaces)	Regulation, proposal of 03.05.22, draft awaiting European Parliament committee opinion, expected by 2025
• Platform Workers Directive	limits monitoring of platform workers' psychological state, private conversations and devices use outside of platform work	Directive, proposal of 09.12.21
Product liability		
• Liability Directive for AI	adapts non-contractual civil liability rules to AI	Directive, proposal of 28.09.22
• Liability Directive for Products	product liability rules extended to cover digital products	Directive, proposal of 28.09.22

* Under EU law, Directives require transposition under national law whilst Regulations are directly applicable

This new 'rule box' is extremely broad, but devils lurk in the detail– a possible maximum 30 day notice period for terminating cloud contracts in the Data Act is a case in point.

22. **Data protection**. The in-house IT lawyer may have responsibility as the organisation's compliance officer for data protection. Particular areas of focus include:
    - establishing the lawful processing basis of all personal data it processes;
    - the organisation's internal and external privacy and data protection policies;
    - demonstrating compliance through records of processing, impact assessments, and privacy by design;
    - operation of procedures and mechanisms for data subject rights;
    - processes and procedures for management of data breaches;
    - appropriate treatment of data protection and data sharing in the organisation's national and international contracts;
    - overseas transfers; and
    - anonymisation.

23. **Cybersecurity**. Organisations are increasingly focusing on a structured approach to their data, network and information security (also known as cybersecurity). This tends to consist of a mix management, legal, technical, operational and governance 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.
    a) **Cyber attacks** are growing in scale, sophistication and consequence, and the impact of each publicised incident is increased by media scrutiny. The NCSC (the National Cyber Security Centre) is part of the UK's GCHQ and reports on cyber threats to business. Major incident trends it currently highlights include:
        - ransomware;
        - DDoS (distributed denial of service) attacks that bombard and overload systems so they fail;

- massive data breaches;
- supply chain infiltration;
- business executive compromise (BEIC) (for example, email scams requesting urgent funds transfers);
- phishing and spoofing and
- cyber crime 'as a service'.

b) **Cyber security, data rights, data protection and data sovereignty**. Security is one of a number of rapidly developing areas of IT 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. They may very briefly be summarized as follows:

- ***cybersecurity***: the legal, technical, operational and governance controls that an organisation puts in place to ensure desired cloud data security outcomes;
- ***data rights***: the intellectual property and other rights that arise in relation to data;
- ***data protection***: the legal rights and duties that arise in relation to personal data;
- ***data sovereignty***: the right of a person to control access to their data by a third party (generally a state agency); and
- other ***data regulation*** for example relating to non-personal data or in particular industry sectors like healthcare, financial services and the public sector.

c) **The NIS Regulations**. In addition to UK data protection legislation (such as the UK GDPR), 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 processed by those systems. 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.

24. **Sector specific regulation**. In addition to generic regulation, if the organisation operates in an area like financial services, healthcare, travel, legal services or utilities, it will be subject to its own sector's regulatory regime. As IT increasingly becomes the beating heart of business, sector-specific regulation will apply more closely to the organisation's IT operations. Special regimes may apply for outsourcing,

the cloud, other critical IT, regulatory audit and reports, and treatment of data or information security breaches, as well as general prudential rules about management and system controls. At least some of these are likely to be within the remit of the in-house IT lawyer.

F. IT GOVERNANCE

25. **Governance**. Along with IT contracts and IT 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 IT 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. Increasingly, organisations are focusing on governance through the lenses of data and Tech as assets and liabilities and the risks that they expose the organisation to.

    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.

26. **Technical standards**. The International Standards Organisation (ISO) publishes an array of technical standards relating to governance issues including:

    - The ISO/IEC 27000 family of standards for information security management;
    - The ISO/IEC 29000 family of standards for privacy;
    - ISO/IEC 38500 on IT Governance;
    - ISO/IEC 38505 of governance of data; and
    - ISO/IEC 56000 on innovation management.

27. **Policies**. IT related areas where the organisation is likely to have been considering specific policies include the following:

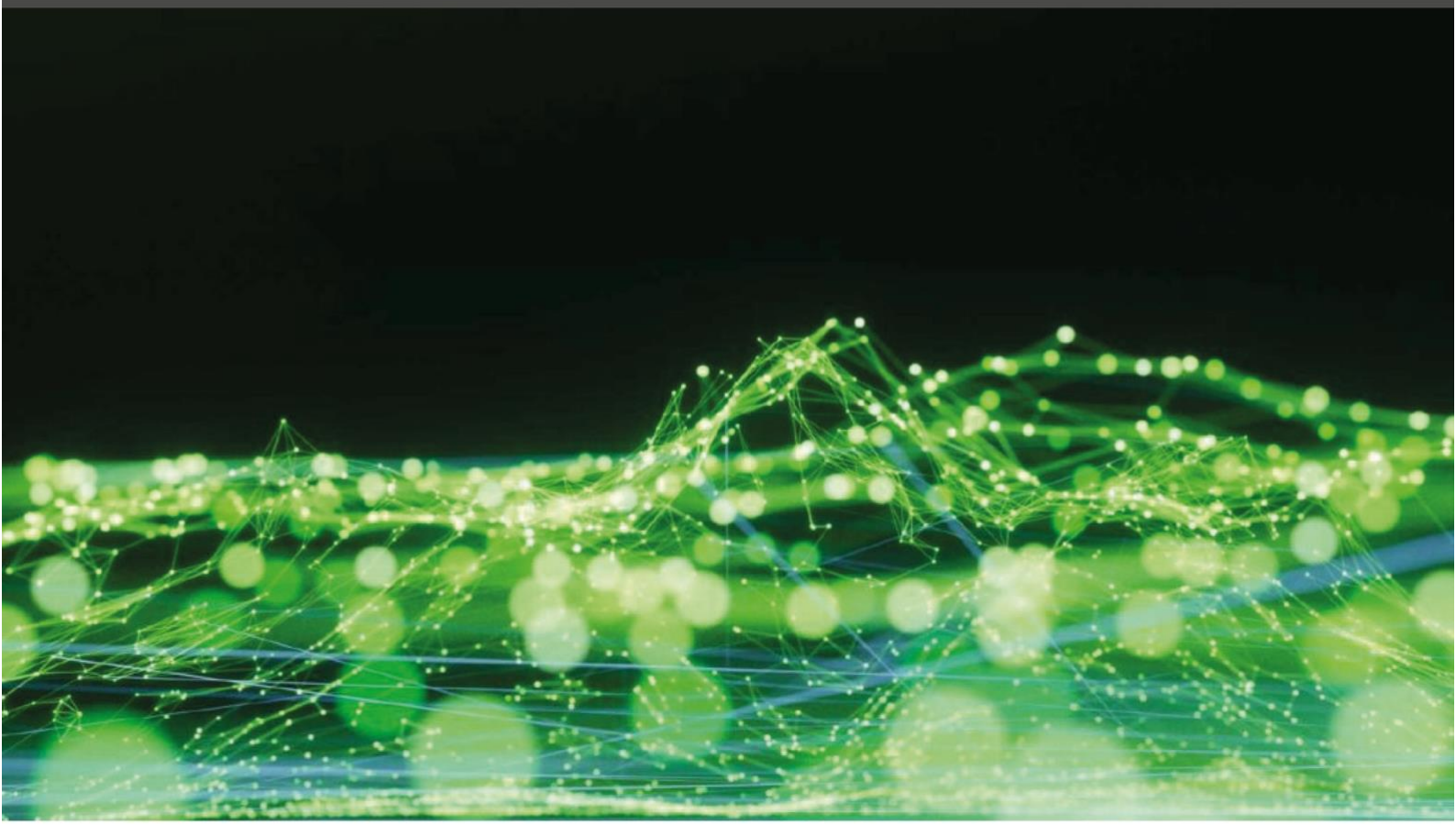
    - IT usage;
    - Privacy/data protection/fair processing;
    - Data security;
    - 'Bring your own device';
    - Monitoring at work;
    - Homeworking;
    - Social media;

28. **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 IT governance and related matters are dealt with on the risk register.

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)