Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Technology & Outsourcing 2022

Definitive global law guides offering comparative analysis from top-ranked lawyers

UK: Law & Practice

Richard Brown, Louisa Chambers, Adam Wyman and Michael Ross
Travers Smith LLP

practiceguides.chambers.com

UK

Law and Practice

Contributed by:
Richard Brown, Louisa Chambers, Adam Wyman and Michael Ross
Travers Smith LLP see p.20

Contents

1. Market

1.1 IT Outsourcing

The IT outsourcing industry remains strong, with organisations continuing to seek the safest and most cost-effective ways to grow, scale and progress. Cost reduction remains a major reason for IT outsourcing, as well as enabling scalability to business needs, improving customer experience and supporting innovation. The COVID-19 pandemic underscored how critical it is for businesses to utilise technology-based solutions effectively and reinforced their symbiotic relationships with IT service providers. Companies that were able to facilitate remote working on short notice were able to limit the impact of the pandemic on their operations and those that faced difficulty in doing so turned to IT service providers for support.

However, despite many businesses learning to rely on cloud-based services and automation, the fallout from COVID-19 is also signalling a return to basics and a renewed focus on cost and risk-management. Cybersecurity continues to be a top concern and emphasis on business continuity has reinforced the importance of strong and reliable partnerships. This has resulted in a growing trend towards developing deeper relationships with fewer IT service providers and the market remains highly competitive. According to a recent survey by PA Consulting, 35% of UK organisations currently outsource their cybersecurity functions; the energy and utilities sector has the highest level at 62%, whereas only 24% of public sector organisations outsource their cybersecurity functions.

Data protection remains a key issue for tech outsourcing. The end of the Brexit transition period at 11pm UK time on 31 December 2020 heralded a shift to a new trading relationship with the EU, based on the UK-EU Trade and Cooperation Agreement (TCA), signed in December 2020. There had been concern that exchange of personal data with the EU would be disrupted, but this was largely avoided through a combination of a six-month grace period in the TCA and the EU's decision that UK data protection legislation offers adequate protection for EEA personal data (which allows it to be transferred to the UK without the need for additional steps, such as use of standard contractual clauses – see **2.3 Legal or Regulatory Restrictions on Data Processing or Data Security**). The UK government has singled out data protection as an area it wishes to reform following Brexit and has put draft legislation before Parliament. However, at the time of updating (October 2022), there were indications that a rethink might be underway, which could result in significant changes. A key concern for outsourcing arrangements will be whether any changes could put the EU's decision on the adequacy of the UK's data protection framework at risk, necessitating additional steps as outlined above.

Inflation is having a major impact on the cost of living, but also on the IT outsourcing industry. Wage inflation and cost increases will affect those suppliers who cannot find a way to pass on these costs. IT contracts are typically shorter, with more flexible termination and/or charging rights; however, now more than ever there will be a focus on payment mechanisms and indexation clauses.

Lastly, the introduction (as a result of Brexit) of a new UK points-based immigration system is making it more difficult and costly for UK outsourcing providers to recruit staff from the EEA. This has an impact across a wide range of sectors, including services requiring technically skilled staff such as computer programmers.

Businesses employ various ways to obtain skills from overseas workers, including entering into a form of agency agreement with an overseas business which then provides developers from all over the world, rather than the classic "outsourcing" model.

1.2 Business Process Outsourcing (BPO)

Despite the increase in IT adoption, dampened business capital expenditure and weak confidence in the global economy has reduced overall demand in other markets, such as business process outsourcing (BPO). The ongoing economic uncertainty since the EU referendum and the start of the COVID-19 pandemic has both reduced demand from some of the industry's major markets, such as manufacturing and retail, and weakened the ability of businesses to invest in future operations. Nevertheless, the drive to source efficiencies in business operations and supply chains continues to support the procurement of outsourcing service providers in all industries.

Notwithstanding the slowing growth of BPO in the private sector, demand from the public sector has risen in the last 18 months. Government contracts are a significant source of revenue for the industry, driven in part by spending in response to the pandemic. However, inflation will also impact BPO, and it is likely there will be an increased focus on payment mechanisms in this area.

The location of service providers has also shifted, with "nearshoring" being an increasingly popular alternative to offshoring. Nearshoring is a form of outsourcing where companies partner with a service provider in a country in the same region. For example, countries such as Romania and Bosnia have become nearshoring centres for business in Western Europe. However, despite cited benefits of nearshoring being cultural familiarity and mitigated risks, it is expected that offshoring is likely to remain the most cost-effective, and therefore popular, solution.

Changes to the UK immigration system, as outlined in **1.1 IT Outsourcing**, continue to make it challenging to recruit staff, including call centre staff.

1.3 New Technology

Robotic process automation (RPA) and cloud-based services continue to have a major impact on the outsourcing sector. Despite high initial set-up costs, automation is often considered a solution for improved productivity, increased employee satisfaction and enhanced customer experience. However, adoption of RPA through outsourcing is becoming increasingly sophisticated, shifting to a more granular focus on overcoming implementation challenges and developing smarter solutions. The use of artificial intelligence (AI) is also becoming widespread, with much higher acceptance than in previous years and businesses in diverse sectors, such as insurance and hospitality, looking to AI to optimise business processes and operational efficiency through automated hiring processes, training, and data analysis.

As regards cloud computing, a survey by Deloitte in 2021 found that 90% of participants saw cloud-based solutions as one of their primary enablers. The COVID-19 pandemic has accelerated cloud adoption further as business operations have been forced off in-house networks and onto the internet. However, data security is still the most cited concern relating to cloud services and additional worries regarding compliance and regulation risk have displaced those relating to performance. The rising number of cyber-attacks are requiring outsourcing provid-

ers to invest heavily in cybersecurity, in order to improve cloud-data security and provide appropriate levels of assurance to their customers.

2. Regulatory and Legal Environment

2.1 New Legal and Regulatory Restrictions on Technology Transactions or Outsourcing

Although the UK regulates the employment aspects of most outsourcing and M&A transactions (see **5. HR**), it does not have any other overarching legislation that seeks to regulate outsourcing transactions on a non-sector-specific basis. That said:

- businesses should be mindful of regulations specific to their industry sector that might have an impact on the outsourced service and the way it is carried out, service levels and other contractual obligations (see **2.2 Industry-Specific Restrictions**);
- public sector outsourcings can be subject to rules on public procurement (see **2.2 Industry-Specific Restrictions**); and
- although relatively rare in practice, certain outsourcing arrangements may be subject to EU or UK merger control legislation; please refer to the Chambers Global Practice Guide: Merger Control 2022 for further information in this regard, and this guide also explains that the UK government has enacted new legislation enabling it to review a wide range of transactions – including certain outsourcings – on the basis that they may give rise to risks to national security.

As noted in a number of cases below, the UK's departure from the EU may lead to changes in regulation, as the UK may decide to diverge from the EU in some areas. In the majority of cases, this is expected to be an evolutionary process which will take time to implement (requiring consultation with industry and the passing of new legislation).

2.2 Industry-Specific Restrictions

Financial Services

Outsourcing transactions relating to financial services are subject to sector-specific regulation, as outlined below.

Regulatory authorities

The majority of financial services firms in the UK are regulated by the Financial Conduct Authority (FCA). Some of those firms (such as banks, large investment firms, insurers, building societies and credit unions) are also subject to prudential supervision by the Prudential Regulation Authority (PRA). The FCA and the PRA have each published specific and detailed rules governing outsourcing arrangements entered into by regulated firms, although the provisions vary depending on the type of financial services business undertaken. Firms that are regulated only by the FCA will need to comply with the FCA outsourcing rules relevant to their type of firm, while firms that are regulated by both the FCA and PRA must also comply with the relevant PRA outsourcing rules. However, note that since a number of rules in this area are derived from EU law, such provisions may be subject to future changes following the UK's departure from the EU.

Oversight

It is a key principle that a firm remains responsible for compliance with any applicable regulatory rules in connection with any outsourced services. This means that the firm will need to exercise proper oversight and monitor the performance of outsourced service providers to verify that any relevant regulatory requirements are

being satisfied. Where the firm fails to do so, it may be subject to enforcement action. The FCA and PRA outsourcing rules typically require the firm to carry out due diligence on any proposed service provider to ensure that the provider has the capacity to provide the necessary services effectively. In addition, the firm will normally be required to ensure that the outsourcing contract contains certain mandatory provisions such as those relating to ongoing co-operation and/or enhanced termination rights.

Where a firm proposes to enter into, or to make significant changes to, a material outsourcing arrangement (broadly where any failure or weakness in the outsourced services might cast serious doubt upon the firm's continuing satisfaction of the conditions for authorisation or compliance with the general regulatory principles applicable to it), it is normally required to provide advance notification to the relevant regulator.

Critical Third Parties

There are also currently proposals for third parties that provide critical services to financial services firms to be subject to direct regulation by financial services supervisory authorities. This would generally be in cases where a failure in, or disruption to, the provision of the relevant services by that third party is considered to have the ability to threaten the stability of, or confidence in, the UK financial system. Such regulation would potentially include a requirement for the third party to meet minimum resilience standards and enforcement powers for the financial services supervisory authorities.

Public Sector Outsourcings

Depending on the nature of the contract and its value, a public-sector outsourcing can be subject to UK public procurement rules (although these apply to a wide range of contracts, not just outsourcing transactions). For example, the awarding authority can be required to advertise the contract, observe certain timings with regard to responses to tender etc, and ensure that all bidders are treated equally and without discrimination. Public procurement rules are most likely to have a significant effect on the timing of the pre-contract procedure, the criteria for selection of successful tenderers, and the duration of the outsourcing contract.

Following the UK's departure from the EU, the UK government identified public procurement as an area it wished to reform. At the time of updating (October 2022), draft legislation had been put before Parliament but the likely timing of its coming into force remained unclear. Whilst the legislation is likely to make some aspects of public procurement more straightforward, the reforms are likely to be more evolutionary than revolutionary.

In the meantime, existing UK public procurement legislation (which is largely EU-derived) continues to apply. It should also be borne in mind that, owing to the provisions of the Brexit Withdrawal Agreement, EU public procurement rules continue to apply to certain transactions, for example, tender processes commenced on or before 31 December 2020 or awards made under framework contracts where the tender process (for the framework itself) was commenced on or before that date.

Critical Infrastructure and National Security

Organisations supplying critical national infrastructure (for example, in sectors such as electricity supply, oil and gas, water, transportation, healthcare and digital infrastructure, including cloud computing storage providers) and meeting certain size thresholds are subject to the Network and Information Systems Regulations (the

NIS Regulations). In brief, the NIS Regulations require such organisations to take appropriate and proportionate technical and organisational measures to manage the security risks posed to them (eg, by taking appropriate measures to protect against cyber-attacks).

Where organisations are outsourcing the provision, management or maintenance of any element of the systems on which they rely to provide such infrastructure, they will need to consider how to ensure that the outsourced activities continue to meet the standards required by the NIS Regulations.

More generally, as noted at **2.1 New Legal and Regulatory Restrictions**, outsourcings involving critical infrastructure and other matters regarded as important to UK national security may be subject to scrutiny under the National Security and Investment Act 2021.

Other Sectors

The parties to an outsourcing will also need to consider any relevant sector-specific regulations, such as requirements for licences or authorisations. These are not normally intended to regulate outsourcing per se, but more to regulate the activity which is covered by the outsourcing. In the UK, the sectors listed below are subject to industry-specific regulation by the regulator listed in brackets:

- aviation (Civil Aviation Authority);
- consumer credit (Financial Conduct Authority);
- education and childcare (Ofsted);
- energy (Ofgem);
- food (Food Standards Agency);
- gambling (Gambling Commission);
- health and social care (Care Quality Commission);
- medicines and medical devices (Medicines and Healthcare Products Regulatory Agency);
- pensions (Pensions Regulator);
- premium-rate telephone services (Phone-paid Services Authority);
- rail (Office of Rail and Road);
- road transport (Driver and Vehicle Standards Agency);
- security services (Security Industry Authority);
- telecommunications, broadcasting and postal services (Ofcom); and
- water and sewerage services (Ofwat).

This list is not exhaustive and the activities covered by the outsourcing may mean that there is a need for licences, permits or approvals from other bodies such as local authorities, the Health and Safety Executive or government departments (for example, certain defence or security-related activities may require Ministry of Defence approval or be subject to review under the National Security and Investment Act 2021).

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

Data protection laws are likely to apply where the outsourced services require the supplier to process personal data on behalf of the customer. “Personal data” includes any data such as names, contact details, or other data which relates to an identified or identifiable natural person. In the UK, at the time of writing (October 2022), the relevant laws are the UK GDPR (which is based on the EU’s General Data Protection Regulation or GDPR) and the Data Protection Act 2018 (Data Protection Laws). That said, EU GDPR will continue to apply to those organisations which fall within its territorial scope. In the UK, Data Protection Laws are enforced by the Information Commissioner’s Office (ICO).

Many outsourcing arrangements, in particular business process outsourcings and IT outsourcings, are likely to result in the handling by the supplier of personal data on behalf of and in respect of which the customer is the data controller – ie, the entity that determines the purposes and means of processing of such data. The supplier will be a processor in such situations. Where this is the case, as well as the supplier having a number of direct obligations to comply with under the Data Protection Laws, the customer must also be satisfied that the supplier will implement appropriate technical and organisational measures to ensure that the supplier's processing of such data will meet the requirements of the Data Protection Laws – in particular, to keep the data safe and secure. The customer must carry out due diligence on the supplier to be satisfied of this. In addition, the Data Protection Laws also stipulate that if the supplier is processing personal data on behalf of the customer and in its capacity as a data processor, the contract between the customer and the supplier must address certain issues (see **4.5 Contractual Protections on Data and Cybersecurity**), namely, requiring the supplier to keep the data safe and secure, and to help the customer in complying with its own obligations, for example, when data subjects seek to enforce their rights in respect of data held by the supplier on behalf of the customer. In some outsourcing arrangements, in particular some business process outsourcings such as pensions administration, it may well be the case that the nature and manner of the outsourced services requires the supplier to effectively act as a data controller in respect of any data it processes, and if this is the case, then the supplier will have to comply with obligations placed on it by Data Protection Laws in its capacity as a data controller.

Overseas Transfers of Personal Data

Personal data transferred to the supplier for processing outside UK must be exported in compliance with the Data Protection Laws, essentially to ensure that the standard of protection for such data under Data Protection Laws travels with the data. This issue will need to be addressed, for example, where the outsourcing involves "offshoring" of service provision to a territory outside the UK. Similar rules apply to customers that fall within scope of EU GDPR and where data will have to be transferred to a supplier located outside the EEA. If the country in which the supplier is located has not been granted an adequacy decision by the UK (essentially, finding that the data protection laws of the destination country are judged to be adequate by the UK government, and meaning that the data can flow freely to the supplier without the need for additional measures to be put in place to protect it), then an alternative safeguarding mechanism will need to be relied on.

The most commonly used safeguarding mechanism is to incorporate a set of "standard contractual clauses" (SCCs) pre-approved by the European Commission (in the case of the EU GDPR) or Parliament (in the case of the UK GDPR). These essentially require the supplier to put measures in place to make sure that they keep personal data safe. The use of SCCs must be supported by a transfer risk assessment. Broadly, this requires the parties to carry out due diligence and a risk assessment to ensure that the laws and practices of the supplier's country provide an equivalent standard of data protection to those in the UK or EEA (as applicable), in particular when it comes to access by public and surveillance authorities to personal data. Account must be taken of the nature of the data being transferred and how it will be processed. Due diligence must also be conducted into the

measures the data importer (in this case the supplier or outsourcing provider) will take to keep the data safe and secure. In some cases, the transfer risk assessment might lead the parties to conclude that the data transfer element of the outsourcing will need to be suspended, and the data kept onshore; it is therefore worth considering this issue early on in the transaction.

Following the ICO consultation in 2021, the International Data Transfer Agreement (IDTA) and the Addendum came into force in March 2022 in relation to data transfers to third countries subject to the UK GDPR. In June 2021, the EU adopted its new SCCs. The UK Addendum is a "bolt-on" to the EU SCCs.

In some cases, alternative mechanisms or specific derogations may be available for transferring the data; for example, suppliers may have obtained approval from the ICO for binding corporate rules that allow them to export data to other group companies based outside the UK, without the need for specific contractual arrangements governing the transfer. Alternatively, it may be possible to obtain the express consent to the transfer of the data subjects whose data is being transferred.

Issues during negotiations

The Data Protection Laws also potentially have an impact at the point when an outsourcing contract is being negotiated, as personal data will be transferred in respect of employees who are transferring over from the customer to the supplier. In these circumstances, care needs to be taken to ensure that personal data is shared and transferred in a lawful manner, with a clear legal basis under the Data Protection Laws for such a transfer. Any personal data transferred outside the UK will again need to be transferred using one of the transfer gateways or derogations outlined above.

Critical infrastructure

As outlined in **2.2 Industry-Specific Regulations**, organisations that supply critical national infrastructure (eg, electricity, oil and gas, water, transportation, healthcare and digital infrastructure, including cloud computing storage providers) and meet certain size thresholds are subject to the NIS Regulations. These regulations may have an impact on the outsourcing of activities relevant to the provision of such infrastructure. For example, where handling of data is outsourced, even if it is not "personal data", the customer will be required to ensure that the supplier takes appropriate measures to protect against cyber-attacks.

Penalties for breach of such laws

The ICO can impose civil fines of up to GBP17 million, or 4% of the breaching undertaking's annual worldwide turnover in the preceding year, for the most serious breaches of the Data Protection Laws. In the case of breach, the ICO can also issue an enforcement notice against a business requiring it to take (or refrain from taking) specified steps in order to comply with the Data Protection Laws.

The Data Protection Laws contain a number of criminal offences, notably offences relating to the unlawful obtaining of personal data and selling or offering to sell such data.

It should be noted that individuals can lodge complaints with the ICO in respect of alleged breaches of the Data Protection Laws and bring an action for damages against the relevant business. Fines may also be imposed for data breaches under sectoral regulatory regimes, for example, financial services firms have been

fined substantial sums for failure to keep customer data secure.

The maximum penalty for breach of the NIS Regulations is GBP17 million, again for the most serious breaches. As with the Data Protection Laws, competent authorities under the NIS Regulations can issue enforcement notices and also have powers to investigate and audit compliance of organisations which fall within the scope of the regulations.

3. Contract Models

3.1 Standard Supplier Customer Model for Outsourcing

Outsourcing can take a number of forms in the UK. Although there is no "standard" model, a direct outsourcing is the most common structure adopted by the parties. This allows a customer to streamline its operations to focus on its core activities, taking advantage of economies of scale available to the supplier as well as the supplier's expertise.

A direct outsourcing is the simplest of the outsourcing structures, with the contract(s) being directly between the customer and the supplier. However, the outsourcing will become more complex if the customer procures the outsourced services on behalf of itself and group companies. In this case, an "agency" model is often adopted, or a third-party rights clause may enable group companies to have directly enforceable rights.

Direct outsourcings typically comprise a single contract (or sometimes multiple contracts) dealing with the core issues (eg, service standards, price, duration, limitations on liability and subcontracting), with schedules setting out (amongst other things) a description of the services provided, service levels, the consequences of failing to meet service levels, governance arrangements and any transferred assets and staff. If the supplier does not have sufficient assets to meet its contractual liabilities or is not the main trading entity in the group, the customer may require a parent company guarantee (see **4.1 Customer Protections**)

3.2 Alternative Contract Models for Outsourcing

Other contractual models commonly used for outsourcing include indirect outsourcing, multi-sourcing, joint ventures or partnerships, outsourcing via a captive entity and build-operate-transfer structures.

Indirect Outsourcing

An indirect outsourcing is similar to a direct outsourcing, except that the customer appoints a supplier (usually domiciled in the UK) that immediately subcontracts the services to a different supplier (usually domiciled in a foreign jurisdiction). The principal reason why a customer may choose this model is that it will wish to interface with, monitor, and enforce its rights against a UK-based supplier, rather than a foreign supplier.

Multi-sourcing

Multi-sourcing is where the customer enters into contracts with different suppliers for separate elements of its service requirements. An advantage of this model (in addition to those achieved with a direct outsourcing) is to avoid being over-reliant on a single supplier, although this only applies where identical services are sourced from several different suppliers. However, maintaining an effective interfacing between the various suppliers to ensure a seamless overall service (ie, Service Integration and Management or

SIAM) can add additional cost and complexity. The outsourcing contract will typically impose contractual obligations on suppliers to co-operate with one another and to participate in a common governance process, involving regular meetings between all of the parties.

Joint Venture or Partnership

The setting up of a joint-venture company, contractual joint venture or partnership to provide services enables the customer to maintain a greater degree of control than the other legal outsourcing structures, to benefit from the supplier's expertise and to share in the profits generated by the third-party business of the joint venture. Joint ventures can take many forms and are usually complicated (and expensive) to set up and maintain.

Captive Entity

A captive entity model is where the customer outsources its processes to a wholly-owned subsidiary to provide the outsourced services exclusively to it and takes advice from local suppliers on a consultancy basis. This model is sometimes known as a "shared services division" if the captive entity is servicing different divisions of the same conglomerate company. Whilst this structure will give the customer greater operational control, possible tax benefits and integration with the supplier/group company, the customer will not be passing the risk of performing the services to a third-party provider, and the upfront set-up costs and ongoing costs are likely to be significant.

Build-Operate-Transfer

A build-operate-transfer model of outsourcing is where the customer contracts a third-party supplier to build and operate a facility, which is then transferred to the customer. It is possible that the customer may ask the supplier to operate the facility for the longer term. Whilst this model is low risk, it can be expensive.

3.3 Digital Transformation

Outsourcing to, for example, cloud-based providers is essentially a form of direct outsourcing; as such, this trend has not, in the majority of sectors, produced any radically new contract models. However, it has had a significant impact on the terms on which services are outsourced. Suppliers such as cloud providers are typically unwilling to negotiate contracts which are, to a significant degree, tailored to the customer's individual needs. This is usually because such an approach would undermine their ability to achieve significant economies of scale by offering a broadly standardised service to a large number of customers, and the argument for imposing standard terms is particularly strong for public cloud services (whereas private cloud services are closer to a traditional outsourcing deal). While contract models have tended to become more standardised and customers have more limited scope to secure contractual protections which reflect their own individual needs and preferences, as the market has matured and become more competitive, it has opened up some (still limited) opportunities for negotiation in key areas.

4. Contract Terms

4.1 Customer Protections

Common protections for the customer in an outsourcing contract include service levels or key performance indicators (KPIs) in relation to the standard of performance of the services. These are typically set out either in the outsourcing contract itself or in a separate "service level agreement (SLA)" appended to the contract. They will generally be linked to obligations on

the supplier in respect of monitoring and reporting on service levels, often combined with audit rights for the customer.

If the supplier does not meet the specified service levels set out in the contract, the contract may provide that the customer is entitled to financial compensation in the form of service credits or liquidated damages. From the customer's perspective, the effectiveness of a service credits/liquidated damages regime depends on two main factors. First, the customer must ensure that the service levels/KPIs measure the aspects of performance about which it is most concerned – otherwise it may have no meaningful remedy at all under the service credits/liquidated damages regime. Second, the service levels/KPIs need to reflect a satisfactory standard of performance; if they can still be met even when the practical outcomes, from the customer's perspective, are sub-standard, then they will not provide a meaningful level of contractual protection. It is also important that the relevant service levels/KPIs are sufficiently precise and objectively measurable.

Given the potential weaknesses in any service credits/liquidated damages regime, customers will usually want to consider additional forms of contractual protection. These will typically include undertakings given by the supplier, including an undertaking that it will provide the services with reasonable care and skill, in accordance with good industry practice and all applicable laws and regulations. The supplier could also be required to warrant the accuracy of information provided by it as part of the tender process, that it has particular accreditations or that it operates in accordance with a particular quality assurance system. If these undertakings or warranties are breached by the supplier, the customer would then be entitled to pursue a claim for damages.

The customer could also seek indemnities from the supplier in respect of specified loss, such as loss suffered by the customer as a result of the supplier's breach of applicable laws, including data protection laws, or against future liability in respect of employees transferred to the supplier as part of the outsourcing (see **5. HR**). Additionally, the customer may require a supplier of outsourced services to hold certain insurance, including in respect of damage to persons or property, and to note the customer's interest on its policy. It is also important for obligations to be imposed on the supplier to maintain a "business continuity plan" and make adequate back-up and disaster recovery arrangements.

In addition, the customer may seek a parent company guarantee (PCG) to secure the performance of the supplier's obligations under the contract if there is any concern that the supplier may not have sufficient assets to meet its liabilities under the contract or is not the main trading entity in its group. The customer may also require the supplier to provide an annual statement (in the form of a board minute) confirming that its directors consider that it can fulfil its obligations under the contract (and it may request the same from the supplier's parent company in respect of the latter's obligations under the PCG).

Whilst these contractual protections will allow the customer to seek compensation from the supplier for failure to comply with the contract, they do not specifically address under-performance. As a result, it is not uncommon for a customer to seek "step-in" rights, allowing it to take over the management of an under-performing service or to appoint a third party to manage the service on its behalf. Less serious problems with

under-performance can sometimes be resolved through use of rectification plans, contract management and governance provisions, which typically require the supplier to appoint a contract manager who will meet regularly with the customer's representative to discuss and seek to resolve issues in accordance with a rectification plan. These provisions may also include a right for the customer to veto proposals from the supplier to dispose of key assets or re-deploy key staff involved in the provision of the services – thereby preventing any deterioration in performance that might be caused by such disposal/re-deployment.

Rights of termination in a variety of circumstances should also be included to protect the customer (see **4.2 Termination**). In addition, customers should ensure that, in the event of termination, the supplier remains under an obligation to provide assistance to the customer in migrating the service to a new provider. As part of this, the supplier should be required to draw up an "exit plan" at the outset of the contract and update it on a regular basis (at least annually) in consultation with and/or with the consent of the customer.

4.2 Termination

Under English law, parties have considerable freedom to decide on the circumstances in which a contract can be terminated. For example, a customer may seek a right to terminate a long-term outsourcing contract on notice without cause prior to expiry of its term without any compensation being payable (often called a termination for convenience). However, the supplier may not be prepared to grant such a termination right or may insist on financial compensation being payable by the customer in the event of early termination for convenience (which will be enforceable provided that the level of compensation is not out of proportion to the supplier's loss arising from early termination, rather than a contractual penalty).

Express Termination Rights and CIGA

In most outsourcing contracts, both parties will have express contractual rights to terminate the contract if the other party commits a material breach of its terms (typically after the expiry of a cure period) or undergoes an insolvency-related event. However, the Corporate Insolvency and Governance Act 2020 (CIGA) introduced further provisions into the Insolvency Act 1986, including in relation to contracts for the supply of good or services. Under CIGA, clauses that enable a supplier to terminate a supply contract (or change other terms) upon an insolvency or formal restructuring procedure are ineffective. CIGA also introduced a prohibition on terminating a supply contract based on past breaches of the contract once the company enters an insolvency process or restructuring procedure. This will mean that (subject to certain exclusions – eg, suppliers who provide financial services and those who are covered by the existing continuation of essential supplies provisions), suppliers will be obliged under the outsourced supply contracts to continue to supply to a customer once it enters an insolvency or restructuring process, even where there are pre-insolvency arrears. Suppliers will also be prevented from making the payment of such arrears a condition of continued supply. The relevant outsourcing contract may only be terminated if the customer or the appointed insolvency practitioner (eg, if the customer is in administration or liquidation) consents, or with the leave of the court if the court is satisfied that the continuation of the contract would cause the supplier hardship. If the supplier's right to terminate arises after the insolvency or formal restructuring process begins (eg, for non-payment of goods supplied

after that time), then there is no prohibition on termination.

Given how difficult CIGA makes it for suppliers to rely on insolvency termination triggers, suppliers may seek to include earlier triggers so as to permit termination before the "relevant insolvency procedures" contemplated in CIGA, for instance, if the customer gives notice of its intention to appoint an administrator (as opposed to the actual appointment of an administrator). In addition, suppliers may seek to further mitigate the impact of CIGA by including a requirement for the customer to provide ongoing financial information to monitor any signs of distress of the customer and/or review their procedures for responding to late payment by customers to pick up on any potential signs of financial difficulties.

Force Majeure

In addition to the above termination rights, the contract may also contain termination rights in circumstances where a party is prevented from carrying out its obligations under the contract for a specified period due to a "force majeure" event. Force majeure clauses exist in a variety of different forms; as a result, whether a "force majeure event" has occurred is highly fact-specific and depends on the precise drafting of the relevant force majeure clause. The occurrence of a force majeure event does not necessarily mean that a party will be relieved of liability for any failure in performance or delay in performance; again, this will turn on whether the drafting of the clause and factual matrix supports such an outcome.

Partial Termination and Change of Control

The customer may also seek to include a right to terminate where the supplier commits specified service failures and may insist that such termination rights can be exercised in respect of the affected services only, or in respect of the contract as a whole. Another termination right commonly requested by the customer is a right for the customer to terminate upon a change of control or ownership of the supplier. A well drafted change of control clause will also include an obligation for the supplier to provide notice:

- of any prospective change of control (subject to relevant confidentiality obligations); and
- within a specified number of days of any change of control occurring.

Repudiatory Breach

In addition to the express termination rights set out in the contract, under English common law, an innocent party will normally have a right to terminate a contract for "repudiatory breach", where the other party breaches a condition of a contract. A condition of a contract is a term that goes to the essence of the contract – whether or not a term is to be categorised as a condition will be a matter of contractual interpretation in each case.

4.3 Liability

Under English law, only loss that was in the reasonable contemplation of the parties at the time the contract was entered into (as a probable result of a breach of it) is recoverable. Outsourcing contracts will typically distinguish between direct and indirect loss. Direct loss means any loss arising naturally and directly from the breach according to the usual course of things or "ordinary circumstances". Indirect (or consequential) loss refers to loss that does not arise naturally but could have reasonably been in the contemplation of the parties because of special circumstances made known at the time of entering into the contract.

If a supplier breaches the terms of an outsourcing contract and the breach directly results in loss to the customer (including loss of business or profits), or if the customer incurs expenses in remedying the breach or obtaining replacement services, such loss is likely to be recoverable by the customer as direct loss. If, however, the supplier's breach results in the customer incurring liability towards a third party under a separate contract, the terms of which were brought specifically to the supplier's attention during a tender process or during pre-contractual negotiations (but which would not otherwise have been in the reasonable contemplation of the supplier upon entering into the contract), the loss incurred by the customer under the third-party contract is likely to be categorised as indirect loss.

Whether a loss is a direct loss or an indirect loss is ultimately a question of fact which has important implications for both customers and suppliers, as set out below.

The customer in an outsourcing arrangement will usually try to ensure that it is able, under the contract, to recover all direct loss incurred by it (including direct loss of profit, business and revenue). It is often sensible to expressly set out particular heads of loss that are recoverable, to evidence that these are agreed to constitute direct loss.

The supplier, on the other hand, will usually seek to exclude liability for indirect, special or consequential loss, and for loss of business, profit or revenue (including where these constitute a direct loss). Market practice by suppliers is to list specific types of loss that are wholly excluded, with the most common being loss of revenue, loss of actual or anticipated profit and loss of reputation or goodwill.

It is important to note that loss of profits (together with the other categories of loss discussed above) can amount to a direct or indirect loss. Therefore, if a contract excludes the right to recover indirect, special or consequential loss, the innocent party may still be entitled to recover loss of profits that arise naturally and directly from the breach (ie, direct loss). As such, if a supplier wishes to exclude its liability for loss of profits, this should be done expressly and separately from any exclusion of indirect, special or consequential loss.

In practice, the types of loss recoverable under the contract will typically be a matter for negotiation between the parties.

4.4 Implied Terms

Under English law, a contract (including any outsourcing contract) will consist of the express terms agreed between the parties together with any terms that are deemed to be implied, either by usage or custom, the parties' previous course of dealings, common law or by statute.

The most relevant statutory implied terms in relation to outsourcing contracts are those set out in the Supply of Goods and Services Act 1982. These include an implied obligation on a supplier of services to carry out such services with reasonable care and skill, an implied term that the supplier will carry out the service within a reasonable time and an implied term that the party contracting with the supplier will pay a reasonable charge (where the contract is silent on such matters or timing/charges are left to be determined by the parties). However, the outsourcing contract often specifically excludes these terms and replaces them with specific provisions, with the intention that all relevant obligations are set out expressly in the written contract.

Where assets are being transferred, a term will be implied by statute that the party transferring the asset has title to it and is able to transfer it. Where the outsourcing involves supply of goods (eg, an IT outsourcing that includes the supply of hardware to the customer), then terms will be implied that the goods are of satisfactory quality and fit for their purpose.

Implied terms as to title to assets cannot be excluded or restricted. Those relating to satisfactory quality, fitness for purpose and certain other matters can only be restricted where this meets the reasonableness requirement set out in the Unfair Contract Terms Act 1977. Typically, however, most suppliers will seek to exclude these terms and substitute their own alternative warranties.

Beyond these statutory terms, it is comparatively rare for terms to be implied into outsourcing contracts. This is because they are generally documented in a reasonable level of detail and the English courts will therefore have regard primarily to the express terms of the contract. However, there are circumstances in which additional terms could still be implied. The most common of these is where the parties have failed to address certain issues in their written contract; a term may be implied where it is necessary to give the contract "business efficacy". Such interventions tend to be used sparingly by the English courts, which are generally reluctant to be drawn into "writing the parties' contract for them".

It is also possible for terms to be implied based on "custom and usage", ie, normal market practice or where there has been previous course of dealing between the parties. However, these would typically only be relevant where the express terms of the contract do not address the relevant issue in sufficient detail. For example, if an outsourcing contract had expired, but the parties continued to deal with one another without having agreed a new contract, an English court might imply terms similar to those contained in the expired contract (based on the parties' previous course of dealing).

4.5 Contractual Protections on Data and Cybersecurity

The Data Protection Laws (see **2.3 Legal or Regulatory Restrictions on Data Processing or Data Security**) require that certain prescribed provisions are included in contracts with suppliers that process personal data on behalf of the customer, to ensure that minimum security levels are met in respect of any personal data which is processed. These include requirements that the supplier only process data in accordance with instructions from the customer, to assist the customer with achieving compliance with its own obligations to take appropriate measures to ensure security of processing, and to back up its obligations with subcontractors to the extent that they process personal data. Following changes introduced by the UK GDPR, data processors are now directly liable for some infringements. As a result, it is not uncommon to see provisions included in contracts to protect their position; also, given the far higher penalties now available, specific liability apportionment for losses resulting from a breach of contractual provisions (and statutory obligations) is becoming more common.

In some cases, the supplier may be processing personal data as a standalone data controller rather than as a data processor on behalf of the customer (for example, in some contracts for the outsourcing of pension fund administration). In these situations, the contract will usually include clauses requiring the supplier to keep personal data safe and secure, and to comply with its

obligations as a data controller under the Data Protection Laws, particularly in respect of any personal data that the customer may transfer to it or vice versa.

Sector-specific legislation and guidelines (see **2.2 Industry-Specific Restrictions**) also impose requirements in relation to data and cybersecurity (for both personal and non-personal data), which are often flowed down to suppliers within an information security schedule.

4.6 Digital Transformation

Given the points made in **4.5 Contractual Protections on Data and Cybersecurity** about the direct liability of data processors for compliance with certain data protection obligations, cloud-based outsourcing suppliers will often include provisions designed to protect their position. More generally, as noted at **3.3 Digital Transformation**, there is typically less scope when using cloud-based suppliers for customers to negotiate "bespoke" contractual protections. However, regulators, for whom data protection and cybersecurity in the cloud has been a particular focus, are increasingly less accepting of cloud service providers' traditional lack of transparency and refusal to risk-share on data issues. This has forced some providers to improve their standard positions in this area or offer sector-specific addenda that include enhanced protections.

Given the limited opportunity to negotiate terms, it is all the more important for customers to carry out due diligence on potential suppliers in order to confirm that the service provided by the cloud-based supplier will comply with Data Protection Laws.

5. HR

5.1 Rules Governing Employee Transfers

In the UK, most arrangements are governed by the Transfer of Undertakings (Protection of Employment) Regulations 2006 (the TUPE regulations). The effect of the TUPE regulations is that employees who are wholly or mainly assigned to the services being outsourced automatically transfer by operation of law to the new provider of the services.

The TUPE regulations apply to an initial outsourcing, where the customer's employees who are wholly or mainly assigned to the activity being outsourced will transfer to the supplier. They will also apply on a change in supplier, where employees of the outgoing supplier who are wholly or mainly assigned to the services will automatically transfer to the incoming supplier. The TUPE regulations also apply to an insourcing, where the outsourcing is terminated and the activities are brought back in-house. In this situation, the relevant employees would transfer from the incumbent supplier back to the customer.

Where the TUPE regulations apply, the relevant employees will transfer on their existing terms and conditions, with continuity of employment preserved. All accrued employment rights and historic liabilities in connection with the transferring employees will also transfer.

5.2 Trade Union or Works/Workers' Council Consultation

Where the TUPE regulations apply, the outgoing employer (the "transferor") must inform and consult with employee representatives about the transfer. Where the employer recognises a trade union, the appropriate employee representatives will be trade union representatives. If no trade

union is recognised, the employer must either arrange for the election of representatives from the affected employees or consult with existing employee representatives where these are in place, for example, where there is a works council or other employee forum.

The transferor must inform the employee representatives about the fact of the transfer, its timing, the reasons for it and the consequences for employees. Where the outgoing employer envisages taking any "measures", it must also consult the employee representatives about those measures. The term "measures" covers any changes to employees' day-to-day working lives, including changes to terms and conditions or working practices, or plans to make redundancies.

To assist with the transferor's consultation duty, if the transferee proposes any measures that would affect the transferred employees after the transfer, it must notify the transferor of the measures before the transfer. If any of the transferee's existing employees will be affected by the transfer, the transferee must also consult employee representatives of its own workforce.

5.3 Market Practice on Employee Transfers

The TUPE regulations apply by operation of law, and it is not possible to contract out of them. However, in practice, the parties to an outsourcing arrangement will typically allocate the employment risks through warranties and indemnities in the outsourcing contract. It is usual for the parties to allocate the risks on both entry and exit. It is often market practice for the indemnities on entry to mirror those on exit so that, for example, if the supplier has been indemnified for employment risks on entry into the outsourcing, they will agree to indemnify an incoming supplier against the same risks on exit. It is also very common for the outsourcing contract to include provisions regarding matters relating to employees during the term of the contract, including any restrictions on changes to terms by the supplier, requirements to provide a list of employees working on the services, and restrictions on changing the personnel assigned to the services.

Impact of Brexit

The UK's withdrawal from the EU has not led to any significant changes to the HR aspects of outsourcings. That said, as noted in **1.1 IT Outsourcing**, the introduction of the UK points-based immigration system post-Brexit has made recruitment of EEA staff more difficult and costly for UK outsourcing providers. In addition, the longer-term impact of Brexit remains unclear. The TUPE regulations and a number of other areas of UK employment law implement EU law. The UK government has signalled its intention to review all UK laws that implement EU law, with a view to removing anything that does not support UK growth or boost investment. It is therefore possible that changes could be made to the TUPE regulations in due course (and this could potentially include removing them altogether).

5.4 Remote Working

The TUPE regulations cover employees working remotely if they are wholly or mainly assigned to the services being outsourced. Such remote workers would transfer to the new supplier along with any other employees who are wholly or mainly assigned to the services. However, for the TUPE regulations to apply, there must be an organised grouping of employees in Great Britain at the time of the outsourcing (or insourcing or change in service provider). If some or all of the employees are working remotely abroad, the TUPE regulations may not apply, as there may

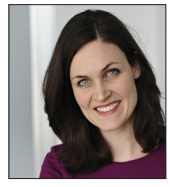
not be an organised grouping of employees in Great Britain.

In general, there is very little regulation on remote working in the UK; this is largely a matter for agreement between an employer and its employees. Many employers will have a policy on remote working, although there is no legal requirement to do so. Employers must, however, ensure they comply with their existing legal obligations in relation to remote workers, including duties relating to health and safety and duties under Data Protection Laws.

Travers Smith LLP has a Commercial, IP & Technology department, which undertakes the majority of the firm's outsourcing work. The department is made up of five partners and 14 associates. The wider outsourcing team also includes specialists from financial services, pensions, real estate, employment and tax who are experts in advising in relation to outsourcing activities and other commercial contracts with third-party providers. Lawyers at Travers Smith advise both customers and suppliers on a regular basis in relation to all types of outsourcings, including IT and business process outsourcing, together with a wide range of other activities which require a more tailored approach, often with an international dimension. The team regularly works across a wide range of sectors, including financial services, retail, warehousing and logistics, pensions, media and publishing and hotels and leisure.

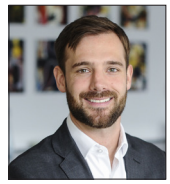
Authors

Richard Brown is a partner in Travers Smith's Commercial, IP & Technology department, specialising in high value commercial contracts and outsourcings. Richard specialises in advising major corporates on key contractual, joint venture and outsourcing arrangements and his clients include household names in the infrastructure, media and retail sectors. He also advises on the carve-out elements of M&A transactions. Richard has developed a fast growing practice in the infrastructure and media sectors, focusing on transactions which are underpinned by long-term contracts, to exploit new markets, opportunities or delivery platforms.



Louisa Chambers is a partner in the Commercial, IP & Technology department and a member of Travers Smith's Technology and Retail Sector groups. Louisa specialises in intellectual property and technology law. She frequently leads major IT projects, such as system implementations and IT outsourcings and advises on all aspects of software, including licensing and the use of open source materials. She also provides regulatory e-commerce and internet law advice to clients with online businesses. Louisa frequently advises clients on cyber-attack and data loss scenarios, advising on general crisis management strategy and notifications to the Information Commissioner and affected individuals.

Adam Wyman is a partner in the Employment department at Travers Smith. He advises UK and overseas employers on a range of employment issues. His experience includes advising employers on the strategy for executive dismissals, board disputes and disputes with current and former employees including senior executive issues and whistle-blowing. Adam runs litigation in the Employment Tribunal and High Court, creates team move strategies and carries out investigations for corporates. Adam leads teams supporting employers carrying out change programmes and advising on the employment aspects of corporate and commercial transactions, including the Transfer of Undertakings (Protection of Employment) Regulations 2006 and redundancy exercises.



Michael Ross is senior counsel in Travers Smith's Commercial, IP & Technology department, specialising in commercial contracts (including outsourcing, supply, distribution, agency and franchising arrangements) and strategic alliances (including joint ventures and collaboration agreements) with experience across a broad range of sectors (including retail, media, logistics, technology, professional services, pensions administration, hotels, brewing, energy and infrastructure). He also regularly advises in support of M&A transactions (including due diligence, transaction documents, transitional services arrangements and complex carve-out/ separation processes).

Travers Smith LLP

10 Snow Hill
London
EC1A 2AL

Tel: 020 7295 3000
Email: commercial@traverssmith.com
Web: www.traverssmith.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com