simmons+simmons

Cloud Services

Contracting guidance

simmons+simmons

Overview

The growing popularity of cloud services has generated questions about the key points in the contractual structure and, for customers new to the cloud market, how best to secure a suitable deal from suppliers. This can be a particular challenge where suppliers believe that a low cost should be reflected in their risk position, whereas a customer is often only too aware that a low-cost deal does not necessarily mean low-risk.

There is no "one size fits all" answer. The term "cloud" encompasses a vast range of services and delivery models. Generally, cloud contracts are service contracts rather than software licensing agreements, and customers may have to change their thinking accordingly. Factors such as this, together with the nature of cloud services, mean that many accepted concepts in traditional IT contracts do not fit neatly into cloud agreements and therefore need to be reconsidered.

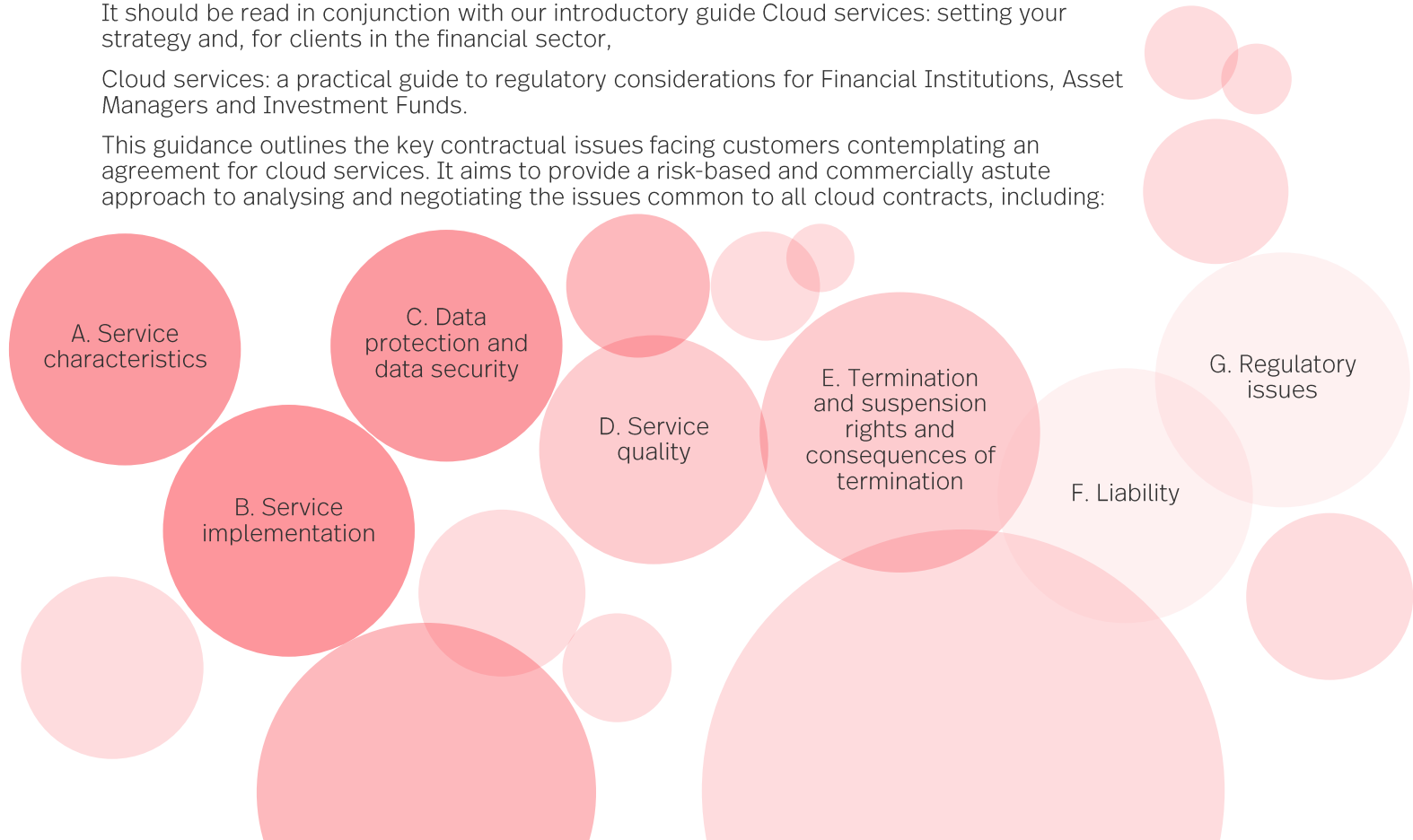
Attempts are being made to fill the gap. The EU Commission has published its own cloud computing strategy and, in June 2014, issued some service level standardisation guidelines. Various regulators, for example the Information Commissioner's Office, the Financial Conduct Authority, and the European Bankers' Association, have also issued guidance on the most important points to consider.

Until recently, large suppliers have been unwilling to deviate from their standard terms. There is, however, evidence that they are prepared to take a more flexible approach, supported by increased sophistication on both customer and supplier sides and the attitude of various regulators within the UK and abroad. This is of course good news for customers and their advisers seeking to drive the best deal.

It should be read in conjunction with our introductory guide Cloud services: setting your strategy and, for clients in the financial sector,

Cloud services: a practical guide to regulatory considerations for Financial Institutions, Asset Managers and Investment Funds.

This guidance outlines the key contractual issues facing customers contemplating an agreement for cloud services. It aims to provide a risk-based and commercially astute approach to analysing and negotiating the issues common to all cloud contracts, including:



How can we help?

We are ideally placed to help you to navigate the challenges that developing and implementing a successful cloud strategy presents as:

We have a combination of customer and supplier-side experience. This means that we have a detailed understanding of where each party's areas of sensitivity may lie and of market norms

We specialise in four client sectors – Financial Institutions, Technology, Media & Telecommunications, Asset Management & Investment Funds and Life Sciences. This means that we have a deep understanding of the regulation and pressures affecting these heavily regulated sectors

We have recent experience on advising major institutions on their internal cloud contracting policies and on cloud services arrangements with the largest suppliers such as Microsoft, Oracle, Workday, Salesforce and others, which means that we can help you to get to the point quickly with those suppliers.

We have supported a significant number of clients in regulated industries on multi-jurisdictional due diligence associated with cloud rollouts and have provided quasi-in-house support on implementing associated compliance measures

Service characteristics

Risk	The services purchased will not actually meet the customer's needs and will fail to deliver the operational benefits expected.
Contractual aim	To achieve clarity of understanding on the part of customer and supplier.
Points to check	**A. Is software to be provided as a service?** If so, the contract should clearly specify the functionality of the software (see also B and C below). Remember that the customer is often completely reliant on the supplier's description of the services. Although the specification is unlikely to remain static, given that the supplier should be obliged to provide enhancements and upgrades over time, the supplier should not have the unilateral right to change the specification in a way which adversely affects the customer. Therefore: ● Any changes to the specification should, ideally, be possible only with mutual agreement – perhaps involving a defined change control process under which changes are proposed, costed and agreed or rejected; ● The contract should restrict the right of the supplier to impose changes which materially impact functionality or use of the services; and ● If the supplier insists on having the right to amend the specification to reflect its overall technology or product roadmap, the customer should consider whether this is acceptable provided it is given the right to see the roadmap and/or a suitable change management process is agreed. **B. Will storage and/or processing capacity be provided, either in connection with the provision of software as a service, or on a freestanding basis?** If yes: ● The description of the storage or processing capacity should be set out together with any applicable limits; and ● Customers should satisfy themselves that arrangements for access and use of the relevant facilities are clear. **C. Will the cloud services include any other material benefits or features and, if so, which ones? (For example, in a software as a service offering, is a test and development environment made available as well as the live production environment?)** If so, a description of these features should be set out in the agreement. **D. Will the cloud services be provided via a private cloud, public cloud or hybrid cloud?** ● If the supplier is providing a dedicated infrastructure (private cloud), this should be specified, using as much detail as appropriate. The use of the expression "private cloud" alone may not be sufficient as it may simply mean a dedicated portion of a "virtualised" server, i.e., a physical server which has been logically divided into a number of "virtual" servers using hypervisor software; ● If the services are to be provided on a non-dedicated infrastructure, the shared elements should be described, together with any spare capacity which the supplier agrees to make available to the customer, and mutual protections for all customers in that space. **E. Will the services available to the customer be easily scalable, for example in the event of changes to the number of service users, the volume of transactions processed, or the required level of storage and/or processing capacity?** If yes: ● is this dealt with contractually? Does it happen automatically? Is there a quick and easy process which the parties must follow to agree scaling at short notice; or must changes be agreed in writing? Are charging structures transparent? ● Can services be scaled down as well as up?

simmons+simmons

Service implementation

Risk	Business interruption if implementation is delayed or is performed poorly
Contractual aim	To give each party clarity about their obligations and provide suitable remedies if implementation does not proceed as planned
Points to check	**A. Will the services simply be "switched on" or will there be an implementation process (potentially including acceptance testing) before they become operational?** **B. If the services are subject to any form of acceptance testing, the following should be set out in the contract:** ● Description of the acceptance testing process, with timescales; ● Acceptance criteria; ● Remedies if any of the services fail acceptance testing or if delays occur. These may take the form of a requirement for the supplier to revise and resubmit the relevant items, and/or rights to terminate the agreement in whole or part for repeated failure or for a protracted delay in acceptance on the part of the customer. **C. Will any adaptation of the supplier's standard "off the shelf" service offering be required?** If yes, customers should make sure that the following is clearly spelt out: ● Any charges for the adaptations or enhancements; ● Ownership of intellectual property rights in the adaptations and enhancements; ● Timing for delivery (possibly linked in to broader implementation arrangements); ● Whether third party adaptations (i.e., which are not created by the supplier or the customer) can be used, and, if so, the process for approval and incorporation and any cost implications.

simmons+simmons

Data protection and data security

Risk	Data breaches, risking liability for fines (up to EUR20,000,000 or 4% of annual worldwide turnover under the EU General Data Protection Regulation) and adverse publicity
Contractual aim	Ensure that customer and supplier understand the importance of compliance and are clear about their respective obligations

Points to check	**A. Will the supplier be hosting or otherwise processing personal data, i.e., data relating to individuals?**
	If so:
	• Which data protection laws apply? (In the EU, this is determined either by (i) whether the controller is "established" in the EU or (ii) if the controller is "established" outside the EU, whether the controller offers goods or services to individuals in the EU or monitors their behaviour.) Once this is clear, advice from local counsel should be sought on the implications for the customer.
	• Will the personal data be hosted or otherwise processed from designated locations?
	  • If yes, the customer should seek specific advice on whether this poses any legal issues from the perspective
	  • of applicable data protection laws;
	  • If no, a "do nothing" approach is not sufficient. The customer should ask the supplier exactly where the processing will be carried out and put in place measures to comply with the relevant data protection laws. (This would affect, for example, a UK customer whose personal data is to be processed in India.)
	• Will subcontractors be involved in the processing of personal data?
	  • If so, details of the subcontractors should be requested from the supplier;
	  • The supplier should be required to ensure that its subcontractors comply with obligations which are no less onerous than those imposed on it, and accept liability for any acts or omissions of the subcontractors as if they were its own; and
	  • The questions above, relating to the locations at which the subcontractors will carry out hosting or processing, should be asked.
	
	B. Will the supplier agree to maintain ISO and other relevant certifications relating to its data security capability, and will it provide copies of its code of conduct, data breach policy and standards relating to data protection?
	• If yes, the customer should ask to see the relevant information, as it may help it to assess whether the supplier's security measures are adequate;
	• If no, the customer should ask why – for example, there may be no legal requirement – and consider whether this is acceptable.
	
	C. Will the customer be able to audit the supplier's compliance with its data protection and data security obligations?
	• If yes, the contract should specify:
	  • The scope of access rights (for example, access to records, data, premises and personnel);
	  • The frequency with which such rights can be exercised (e.g., annually), with exceptions if required by any regulator; and
	  • What happens if an audit reveals failings on the supplier's part – for example, will the supplier be obliged to remedy the issue and/or reimburse relevant charges?
	• If not, the customer should consider how, if at all, it could in the absence of such rights comply with its legal obligations to monitor the supplier's compliance with its data protection duties. This might be an unacceptable risk.

	D. Will the customer be subject to local laws implementing the EU Network and Information Systems Directive or other laws relating to cybersecurity? ● If so, should any requirements over and above those required under data protection law be imposed on the supplier? E. The customer may also wish to establish the extent to which the supplier derives data from customer data on the cloud service, the intended use of such derived data, and the rights the customer has in respect of such derived data. F. The customer may also wish to establish the extent to which the supplier derives data from customer data on the cloud service, the intended use of such derived data, and the rights the customer has in respect of such derived data. G. The customer may also wish to establish the extent to which the supplier derives data from customer data on the cloud service, the intended use of such derived data, and the rights the customer has in respect of such derived data.

simmons+simmons

Service quality

Risk	In any cloud arrangement, the customer will lose some level of control compared with in-house services. Any lack of control which adversely affects the quality of the services could have a significant operational impact for the customer.
Contractual aim	To ensure that adequate quality standards are explicitly set out in the contract and that suitable rights and remedies are available to the customer if those standards are not met

Points to check	**A. Will the supplier offer service level commitments relating to the performance of the cloud services?**
	• If yes, do these commitments cover any or all of the following, as appropriate for the services which are being procured:
	  ◦ Availability of the services, together with the method of measuring availability (for example, by reference to all of the functionality or specified aspects of it only and/or the physical point at which availability is measured (for example, the outer perimeter of the supplier's data centre)). Any maintenance windows must be acceptable in terms of timing and duration;
	  ◦ Response and resolution times for support or helpdesk services;
	  ◦ The speed with which transactions are processed;
	  ◦ Security incident management and reporting (percentage of timely incident reports, responses and resolutions);
	  ◦ Reporting on the supplier's compliance with service levels.
	• If no, this is a potentially serious risk issue for the customer, and it may consider approaching another supplier.
	
	B. Will the supplier allow the customer to audit its compliance with service levels?
	• If yes, similar practical considerations to those in paragraph C of the 'Data Protection and Data Security' section apply.
	• If not, the customer should consider whether the service level regime, read as a whole, provides sufficient comfort for it without these rights (for instance, whether it understands the mechanism for measuring compliance with service levels and considers it to be sufficiently robust and transparent) or whether it should insist on these rights being included.
	
	C. The customer should consider whether other quality-related provisions are appropriate, possibly relating to:
	Capacity
	• The capacity of the services (for example, what is the maximum capacity of a specific element, such as the maximum number of connections to the service; the maximum number of requests that can be processed per minute; the maximum storage, memory or CPUs; and the maximum number of simultaneous users of the cloud service);
	Interfacing and resilience
	• The capability of the services. This will vary between customers according to their intended use of the service but could include, for example, the ability to connect to external third party systems;
	• The resilience of the service, for example the redundancy and reliability of the cloud service supply chain or elements of the cloud service;
	Handover to a replacement supplier
	• The reversibility and termination process (which describes service levels regarding the takeover of the service by a replacement supplier and the termination of the arrangements, for example, the period of time in which the customer can retrieve data, the period of time the data is held by the supplier as back-ups, the period of time residual data about the customer, but not belonging to the customer, is held by the supplier);

Security

- Authentication and authorisation of users of the service - for example, the authentication mechanism used; the assurance given to the mechanism to authenticate a user accessing a resource; the mean time required to revoke user access; user access credentials storage and protection; third party authentication support (namely the extent to which the supplier will support third party authentication or technologies to enable interoperability of identity management solutions between the customer and other providers);
- Cryptography of customer data – describing the encryption methods used so that customers can evaluate different cloud services;
- Logging and monitoring of the cloud services, for example including the logging parameters, the log access availability and periods of time for which logs are available for analysis;

Vulnerability

- Vulnerability management, such as the number of vulnerability corrections performed by the supplier; the percentage achieved within a predefined time limit following notification and full reports on the vulnerabilities addressed; and

Change management

- Matters such as reporting processes for planned changes to services, and the number of notifications of changes made within a predefined time period.

D. What remedies are available to the customer if the specified service level commitments are not met?

These may include:

- Service credits, usually expressed as a reduction in the charges. These may be capped at a percentage of the total charges;
- Termination rights, although these are usually reserved for persistent or one-off catastrophic failures;
- The right to claim damages (subject to financial limitations of liability and exclusion of certain types of loss). Exercise of this right will depend on the customer being able to show a clear breach of a service level, so care should be taken that service levels are expressed clearly and as binding obligations and not merely "targets";
- Practical remedies, such as obligations to remedy or workaround service failures.

E. Are specific contractual remedies (usually service credits and termination rights) stated to be the customer's sole and exclusive remedy for service level failures?

- If yes, the customer will need to consider whether this is commercially acceptable in the light of its potential loss if the cloud services fail to meet the agreed quality levels. It may seek to tip the balance of risk more heavily towards the supplier, possibly by supplementing the right to terminate with other rights of recovery (see Termination and Suspension Rights and Consequences of Termination section) or lowering the threshold at which service credits and termination rights are triggered and increasing the levels of service credits available.

simmons+simmons

Termination and suspension rights and consequences of termination

Risk	The customer is unable to terminate an unsatisfactory arrangement easily, with adverse results on its business; an outgoing supplier is under no obligation to assist in the transition to a new provider and the customer's business continuity is threatened. Separately, a customer may not understand the supplier's suspension rights which might prove commercially disastrous.
Contractual aim	To give the parties a commercially acceptable mechanism for the suspension or termination of services and procure an orderly handover with minimum disruption to the customer's business.

Points to check	**A. How long is the committed term? Does it meet the customer's business needs?**
	
	B. Does the agreement include termination rights, and do these rights apply equally to both parties?
	● If it does, look for typical provisions, such as:
	  ● Rights to terminate for material breach – often giving the breaching party a specified period of time to remedy the breach;
	  ● No-fault termination on notice (is the notice period suitable?);
	  ● Rights to terminate on the insolvency of the other party;
	  ● Rights to terminate on other events such as a change of control of a party or in connection with key areas of the contract, for example data protection, data security or regulatory compliance.
	● If no such rights are included, be aware that the standard common law rights may have been excluded or, even if they remain, may not be adequate, so appropriate provisions should be negotiated.
	● Institutions subject to the EBA Guidelines on Outsourcing will require an agreement which expressly allows for the institution to terminate the arrangement, including in situations where the outsourcing provider is in breach of law, regulation, or contractual provision; where material changes affect the outsourcing arrangement or service provider; where there are weaknesses regarding management and security of sensitive data or information; where impediments exist which are capable of altering the performance of the outsourced function; and where the institution's competent authority requires termination.
	
	C. Does the agreement give the supplier any suspension rights?
	● If yes, the customer should proceed with caution. Rights which apply:
	  ● in "hair trigger" scenarios, for any breach (or suspected breach) of any obligation, including payment obligations, by the customer;
	  ● in scenarios in which the customer is not at fault; and/or
	  ● for an indefinite duration pose a significant operational, commercial and (potentially) regulatory risk for customers. Similarly, the impact of suspension rights on customer obligations to pay charges should be considered and addressed appropriately. There is a strong argument that suspension rights should only apply in the case of contractual breaches by the customer which could have an impact on other customers of the supplier.

D. What are the supplier's obligations on termination or expiry of the agreement? One or more of the following are likely to be appropriate:

- A requirement for the supplier to continue providing the cloud services for a defined handover period, with the customer continuing to be liable for charges during that period. The handover period should be long enough to allow for the customer to migrate to an alternative solution;
- An obligation on the supplier to provide assistance and technical information needed by the customer to enable transition to a new supplier, subject to reasonable confidentiality and intellectual property protections and, potentially, compensation for the work involved;
- A requirement for the supplier to deliver up machine-readable copies of customer data in a format specified by the customer and to cease using customer data, subject to the customer having had opportunity to test the data and validate that it is suitable for use on a replacement platform;
- If termination is triggered by the supplier's insolvency, the supplier should be required to allow a third party to provide "escrow-equivalent" protection. This might, at the very basic level, involve such third party paying the supplier's key sub-contractors (such as hosting or data centre providers) for a period of time, or at a more complex level may involve taking over the running and maintenance of the cloud service as well as payment of sub-contractors (this type of service would need to be established at the outset of the contract). In relation to Software as a Service arrangements, a customer might also wish to explore whether a conventional source code escrow arrangement is available as this could be a practicable way to manage the risk of supplier failure.
- Institutions subject to the EBA Guidelines on Outsourcing should ensure that the agreement clearly sets out the obligations of the existing service provider; sets an appropriate transition period; and obliges the service provider to support the orderly transfer of the function in the event that the agreement is terminated.

simmons+simmons

Liability

Risk	The supplier's liability for failure to deliver the promised service, or for other breaches of the agreement, is excluded or is capped at a level which fails to compensate the customer adequately for the losses and disruption it suffers.
Contractual aim	To provide a risk profile for the contract which is acceptable to both supplier and customer and which is legally enforceable.
Points to check	**A. Does the agreement include limits on each party's liability? (Customers should be aware that such limits could take the form of, e.g., very short windows of time for making claims as well as the more usual financial caps on the amounts that can be recovered.)** **B. Does the agreement completely exclude each party's liability for certain types of loss (for example, loss of profits, goodwill, consequential loss, loss of data or processing time)?** ● If yes, the customer will have to analyse the overall risk profile of the agreement and consider whether these exclusions overly erode its rights of recovery. For example, if data is to be hosted by the supplier, what degree of responsibility and risk should it assume if data is lost or corrupted while under the supplier's control? Are ways to mitigate this risk – for example, data back-ups and/or practical remediation obligations – reflected in the contract, or can they be implemented "outside" the contract, and, if so, at what cost? ● All but the least sophisticated suppliers will include exclusions and having multiple customers on a single system is a very powerful incentive for a supplier to restrict its liability as much as possible. However, a balance needs to be struck between the parties' interests which is appropriate in the commercial context. Typically, a supplier will take a "risk v reward" approach whereas a customer focuses more on full (or substantial) recovery of foreseeable losses. **C. Are there any carve-outs from the limits or exclusions of liability (i.e., areas to which the limits or exclusions do not apply)?** ● If so, are they aligned with those areas which the customer regards as important or high risk, such as confidentiality, data security and third party intellectual property claims? ● Does the supplier offer an indemnity in respect of such matters, and if so are there any conditions imposed on the customer's right to claim under the indemnity? **D. If the contract provides a framework of remedies, how do these work with the general exclusions or limitations of liability?** ● For example, are service credits expressed to be available to the exclusion of a general right to claim damages? Is there an upper limit on the total amount of service credits which are available? In such a case, it is important to look at the contract as a whole. The topic of exclusions and limitations of Liability is a complex one from a legal perspective so specialist advice is recommended.

Regulatory issues

A. Beyond data protection law, is the customer subject to any other specific legal or regulatory requirements which need to be taken into account when contracting for cloud services?	If yes, these need to be reflected in the agreement. For example, financial services regulation may, depending on the nature of the cloud services and importance of them to the customer's business, require that certain points need to be addressed in the agreement or in the procurement process by the customer.
B. How, if at all, are any future changes to these requirements addressed?	For example, is the customer required to make changes to its solution to address regulatory change and will it bear or share the cost impact of all or some changes in law?

Contact us

Alexander Brown
Partner
Information, Communications & Technology
T + 44 207 825 4954
London
E alexander.brown@simmons-simmons.com

Hinal Patel
Partner
Information, Communications & Technology
T + 44 207 825 2080
Bristol
E hinal.patel@simmons-simmons.com

Lawrence Brown
Partner
Information, Communications & Technology
T + 44 207 825 3053
Bristol
E lawrence.brown@simmons-simmons.com

George Morris
Partner
Information, Communications & Technology
T + 44 207 825 4046
London
E george.morris@simmons-simmons.com

James Cotter
Partner
Information, Communications & Technology
T + 44 207 825 3194
London
E james.cotter@simmons-simmons.com

Tom Wheadon
Partner
Information, Communications & Technology
T + 44 207 825 3603
London
E tom.wheadon@simmons-simmons.com

Simmons & Simmons is a leading international law firm with more than 900 legal staff in offices situated in key business and financial centres across Europe, the Middle East, and Asia. We believe it is who we are and how we approach our work that sets us apart from other firms. We set the highest standards for the work we do and pride ourselves on our client focus.

In building our international business, we have created a closely knit and cohesive network of lawyers who seek to balance local business needs with the delivery of a global service. Our current client base includes a significant number of the current FTSE 100 and Fortune Global 500 companies and we advise the world's leading investment banks, many of the world's largest financial conglomerates and more than half of the top 50 European hedge fund managers. We provide services from locations based in Europe, the Middle East and Asia. We work across core practice areas including corporate, dispute resolution, EU, competition & regulatory, employment, pensions & employee benefits, financial markets, intellectual property, projects, real estate, information, communications & technology and tax.

A key commercial advantage for our clients is our focus on specific sectors, including asset management & investment funds; financial institutions; technology, media and telecommunications (TMT); and life sciences. We also focus on the energy and infrastructure market, in particular through our international projects and construction teams.

For additional information on our firm, please visit our website at **simmons-simmons.com.**

L_LIVE EMEA1: 45414901v1