International
Comparative
Legal Guides

Practical cross-border insights into technology sourcing

Technology Sourcing 2022

Second Edition

Contributing Editor:
Mark Leach
Bird & Bird LLP

ICLG.com

ISBN 978-1-83918-206-8
ISSN 2752-6909

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Technology Sourcing 2022

Second Edition

Contributing Editor:
Mark Leach
Bird & Bird LLP

Expert Analysis Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the second edition of *ICLG – Technology Sourcing*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to technology sourcing laws and regulations around the world, and is also available at www.iclg.com.

This year the expert analysis chapters cover contracting for AI solutions, and strategic sourcing across technology and business services.

The question and answer chapters, which in this edition cover 18 jurisdictions, provide detailed answers to common questions raised by professionals dealing with technology sourcing laws and regulations.

As always, this publication has been written by leading technology sourcing lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Mark Leach of Bird & Bird LLP for his leadership, support and expertise in bringing this project to fruition.

James Strode
Publisher
Global Legal Group

ICLG.com

USA


Sean Christy


Chuck Hollis


Derek Johnston


Anne Friedman

Bryan Cave Leighton Paisner LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, however, there are federal and state laws and regulations that may apply to the subject matter or other aspects of the transaction (e.g., data privacy) or industry of the contracting party (e.g., financial services, healthcare).

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The DoD, GSA, and NASA jointly issue the Federal Acquisition Regulation (FAR) for use by executive agencies in acquiring goods and services, and part 39 of FAR describes the terms of acquisition of information technology. The procurement of goods and services by state and local governmental bodies is governed by state procurement laws of the state in question, and for some municipalities, by the applicable municipal code.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, but parties to such a contract will generally agree to contract terms that range from one year to several years, depending on the nature, scope, and complexity of the arrangement.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, the length of any termination notice period and the termination provisions themselves are instead negotiated by the parties on a case-by-case basis in view of the nature, complexity and criticality of the technology-related services and the initial investments incurred by the parties. However, in the consumer context, there are various federal and state laws that may require the supplier to follow certain processes and provide the consumer certain notices before terminating, and the common law of some states may impose a presumptive reasonable renewal term on contracts that the parties continue performing beyond expiration.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

The common law of most states imposes an implied duty of good faith and fair dealing on the parties to a contract. It is not uncommon for a contract to include a more definitive, express covenant for the parties to cooperate and deal with each other reasonably and in good faith to effectuate the purposes of the contract.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Customers are entitled to recover proven, direct damages for breach of contract. The definition of direct damages varies from state to state, with some states having a more well-developed body of common law lending more predictability.

In addition, equitable remedies (e.g., injunctive relief) may be available where monetary damages are not sufficient to make the non-defaulting party whole and other conditions are satisfied, and additional common law remedies (e.g., restitution, rescission, specific performance) may be available.

Technology sourcing contracts frequently include:

- A definition of what constitutes recoverable "direct damages" to lend predictability to the types of damages that are recoverable, including the cost of cover and other foreseeable damages that would result from a breach.*
- A negotiated monetary damages cap on amounts recoverable for breach of contract (typically ranging from 12 to 24 months' fees with outliers in exceptional circumstances).
- Disclaimers of indirect, special, consequential and punitive damages and often of lost profits, reputational harm, diminution in value and similar damages.
- Exclusions from both the monetary damages caps and the disclaimers of indirect damages, often with a separate, higher cap (typically ranging from 24 to 48 months' fees with outliers in exceptional circumstances) for certain types of damages and indemnities (e.g., for data breaches) and with other damages and indemnities not being subject to any limit (e.g., gross negligence and wilful misconduct).

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

These contracts often include a variety of additional remedies and protections depending on the scope and deployment model of the solutions and services, with more customer leverage mechanisms and remedies in outsourcing agreements and much fewer in cloud agreements. Remedies may include:

- The ability to withhold a portion of the fees in a scope dispute.*
- The right to step-in and correct performance failures and to recover the incremental costs of stepping in.*
- The right to set off amounts in dispute* and other amounts owed to a customer against the charges (sometimes subject to an escrow requirement above a certain threshold or, less commonly, an outright cap).
- Service levels and other performance metrics and remedies.
- A defined acceptance process, with no cost repair, cover, and termination remedies for non-conforming transition and other one-time deliverables.
- Milestone payments and sometimes credits to incentivise timely and proper completion of transition services/deliverables.
- A prohibition against intentional breach (abandonment) by the supplier and injunctive relief and enhanced recovery for same.*
- The termination rights described at question 2.7.
- An express obligation for the parties to continue performing during disputes.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

The contract typically provides when a party may terminate. These termination rights will, when properly invoked, enable a party to terminate the contract without giving rise to a claim for unspecified damages from the terminated party, but each party may have claims for damages independent of the termination.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties can, and typically do. Examples include: (1) a customer termination right for convenience (subject to payment of an express termination charge);* (2) a right to terminate for the supplier's (and in rarer cases, the customer's) insolvency; (3) a customer termination right for repeated or significant service level failures; (4) a customer termination right for persistent, uncured breaches;* (5) a customer termination right for a supplier's breach of the agreement's confidentiality or data security requirements; (6) a customer termination right for other material breaches that remain uncured for more than 30 days; and (7) limiting supplier termination rights to customer payment defaults.* A contract may also include certain rights, exercisable by the customer upon termination or expiration of the arrangement, which almost always include a post-expiration/termination wind down period during which the customer can continue to receive the services and request other cooperation to repatriate or transition services to a replacement provider.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

The interpretation and enforcement of clauses that seek to limit a party's liability are generally governed by state, not federal, law. As a general rule, if the parties to a contract are both sophisticated business entities dealing at arm's length, they are free under the laws of most states to negotiate both limits on liability and exclusions from those limitations in their contracts. However, some states view liability limitations in contracts less favourably than others, and the parties should take care in their choice of governing law.

Certain liabilities may not be limited under the common law of many states, typically including the liability of a party arising from its fraud, wilful misconduct and gross negligence and, in some states, the wilful injury to person or property or violations of law (regardless of whether the violations are intentional or not).

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Generally, yes, if the proposed cap on liability: (i) is reasonable in relation to the fees for the services; (ii) generally relates to economic damages arising out of the negligent acts or default performance of either party; and (iii) would not otherwise violate public policy.

In the ordinary course, the amount of the liability cap, the inclusion of super caps or enhanced caps, the application of the liability cap, and any exclusions from the liability cap are among the most heavily negotiated matters in the contract. See also question 2.4 above.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

Not as a matter of state or federal law, but there are special considerations contextually. Cloud contracts and software licence and support contracts are generally less customer-friendly inasmuch as they include fewer customer leverage points (those marked with an "*" above being customarily excluded). By extension, the same limitations would apply to the licence or cloud deployment of AI and blockchain solutions.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Most outsourcing contracts resort first to informal dispute resolution between the parties and sometimes with escalation to management before resorting to more formal dispute resolution – usually litigation or binding arbitration, although sometimes mediation is a precursor to litigation. Software licensing and cloud computing contracts less often include informal dispute resolution, as those contracts are usually less robust as a general

matter. In all cases, the contracts will often specify the federal and/or state courts for the resolution of litigated disputes, taking into account facts relevant to personal jurisdiction requirements under federal and state law. U.S. customers with foreign-domiciled suppliers often prefer arbitration, with the preferred arbitral rules and tribunal varying based upon where the parties are domiciled and other factors. If arbitration is chosen, the parties will usually reserve certain matters for litigation (e.g., equitable relief, confidentiality, intellectual property).

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The intellectual property rights (IP) of each party are typically protected by the terms of the contract and statutory protections for certain IP (e.g., patents, copyrights, trademarks).

The licences and allocation of IP ownership under a contract vary based on the type and scope of services. Typically, the customer and supplier retain ownership of IP that they bring to the arrangement and any improvements or derivative works thereof. For new developments, the scope of the arrangement will dictate the allocation of ownership and any licences to such IP.

Each party will license to the other party its IP that is necessary to perform or receive the services. In certain instances, customers will receive perpetual licences to the supplier's IP, which often relate to IP that is necessary for the customer to continue operations post-termination/expiration (less common in the cloud context) or to IP that is embedded within, or is otherwise necessary for the use and maintenance of, the customer's systems and other deliverables.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Any assignment of IP rights should be in writing and executed by the assignor. The assignment may also require consents from third parties, may be governed by an agreement with such third parties, and may be subject to certain fees or other charges. Trademarks must be assigned with their goodwill in order to be valid. The transfer of patents and trademarks should be recorded in the U.S. Patent and Trademark Office, and copyrights should be recorded in the U.S. Copyright Office.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Generally, know-how, trade secrets and other business critical confidential information are protected by statute and by common law. In particular, 48 states have adopted some form of the Uniform Trade Secret Act protecting trade secrets at the state level. In the other two states, trade secrets are protected by common law. Trade secrets also may be protected under certain federal laws. In most instances, the contract includes language protecting know-how, trade secrets and other confidential information.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

There is no uniform federal law governing the processing of personal data in the U.S., which is instead governed by a patchwork of federal and state laws. At the federal level, the Gramm-Leach-Bliley Act and a patchwork of regulatory guidance by the federal financial institution regulators (applicable to financial services), HIPAA and the HITECH Act (applicable to protected health information), and the Family Educational Rights and Privacy Act (applicable to educational institutions and their vendors), along with their implementing regulations, are the most frequently implicated. Data security and protection requirements at the state level vary significantly, with breach notification laws in all 50 states and some of the more protective privacy regimes existing under the California Consumer Privacy Act/California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the New York SHIELD Act, and the NYDFS cybersecurity regulations. Finally, U.S. customers with international operations remain subject to international privacy laws like GDPR.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

No geographic transfer restrictions apply to personal data generally in the U.S. However, there are some limitations on the transfer of certain data in the custody of certain federal and state agencies (e.g., federal income tax data).

5.3 Are there any legal and/or regulatory requirements concerning information security?

In addition to the more generally applicable requirements referenced in question 5.1, there are industry-specific requirements related to information security. For example, federal guidelines apply to critical infrastructure operators and certain industries (e.g., telecommunications, electrical utilities, transportation, and the public sector) that are subject to federal and state regulations that include information security requirements. Recent examples include:

- Executive Order 14028: Improving the Nation's Cybersecurity was signed by President Biden in 2021 in response to the SolarWinds and Colonial Pipeline incidents and other attacks, and along with subsequent federal regulatory guidance (including various OMB memos that ensued) has implications for future contracts involving the federal government.
- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 imposes breach notification requirements on certain critical infrastructure covered entities.
- In November 2021, the OCC, FDIC and FRB issued the Computer-Security Incident Notification rule, which imposes reporting requirements related to qualifying security incidents on both regulated financial institutions and bank service providers.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

No, in the absence of a collective bargaining agreement or other contractual arrangement, employees in the U.S. are never transferred to a supplier solely by operation of law pursuant to a commercial contract. Employees are generally considered "at will" employees and, therefore, these employees may be terminated at any time for any lawful reason.

6.2 What employee information should the parties provide to each other?

If the customer intends to transfer employees to the supplier, the supplier will need information relevant to making an offer of employment to those employees, including information relating to salary, benefits, years of service and skill sets.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Generally, yes. Employees in the U.S. are considered "at will" employees and may be terminated by an employer for any lawful reason, in the absence of a collective bargaining agreement or other employment contract prohibiting such a termination. Further, the Worker Adjustment and Retraining Notification Act (the WARN Act) and similar state laws require certain employers to notify their employees of mass layoffs, widescale hour reductions or site closures. Employment contracts with certain employees, a prior course of conduct or other existing company policies might also obligate the employer to notify its employees or even to provide severance or other bonuses to employees whose employment is being terminated as a result of a new technology sourcing contract.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, as noted above, under the laws of the U.S., the parties are generally free to negotiate and establish the new employment terms for transitioning employees, subject to any existing collective bargaining arrangements, employee contracts, company policies and/or prior course of conduct.

6.5 Are there any pensions considerations?

Yes, companies that maintain pension benefits for their employees cannot discharge or avoid these benefit liabilities by simply outsourcing the affected services and transferring the in-scope employees. Liability for any existing or future pension benefits is governed and determined by federal law.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Current U.S. law generally accommodates the offshoring of work by U.S. corporations, subject to certain narrow exceptions (e.g., OFAC's Sanctions Programs and SDN List). The purchase of services by a federal or state entity is highly regulated and there may be restrictions on the offshoring of certain services. Multi-jurisdictional contracts may also trigger other laws that limit or apply conditions to transfers (e.g., ARD/TUPE).

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Not generally, but certain federal and state laws and regulations may apply contextually. For example, (i) the regulations mentioned in section 5 above may apply where personal data is in scope, (ii) third-party risk guidance (from the FRB, OCC, FDIC, FINRA, and the NYDFS and other regulatory agencies) may apply in the financial services industry, and (iii) FERPA will govern the scope of permitted outsourcing in higher education. The type of services also may implicate additional laws. For example, the FDCPA, TCPA and other consumer protection laws (e.g., Do Not Call Registry and the CAN-SPAM Act) may apply to outbound contact centre services.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

While there are several common contract structures, the most widely utilised contract structure is a Master Services Agreement accompanied by one or more Statements of Work.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Service levels are commonly included in outsourcing contracts. Each service level is defined in terms of the process or service measured, a unit of quality, and a period of time. Service levels are typically measured on a monthly basis, but may be measured over longer periods of time (e.g., quarterly, annually), or as one-time events.

Service level metrics are set based on the customer's requirements, the customer's historical data or sometimes via baselining. Measurement, monitoring and reporting tools should be specified for each service level. Service level accountability and/or credits may be delayed for a stabilisation period in certain instances.

There are often two or more classes of service levels, and each service level may have a single or multiple targets depending upon the complexity of the methodology. More critical service levels bear credits if the supplier fails to meet the applicable target. Other service levels may be tracked and measured, but not result in credits. Customers usually have the periodic right to reclassify service levels as credit-bearing or not and to reconfigure the allocation of credits across the service levels. In some arrangements, there are other general reporting metrics that are tracked, measured, and reported, but are not eligible to be credit-bearing.

Service level credits are reductions of the fees paid by the customer and are not characterised as penalties, which are generally unenforceable, or as liquidated or exclusive remedies. Rather, service level credits are most often treated as a credit against the customer's damages.

Service level credits are subject to a defined amount at risk (cap). Generally, that amount is defined as a percentage of monthly or annual fees, ranging from 10% to 15%, with outliers in exceptional circumstances. In more complicated transactions, the customer may have the right to over allocate the amount at risk, with the overallocation typically ranging from 150% to 275% of the amount at risk, but aggregate credits are always subject to the amount at risk. In some instances, the supplier may "earn-back" the service level credit for continued performance at or above the target.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Charging methodologies vary greatly. The following are a few examples:

- A methodology based on the volume of resources. This method may include a fixed charge with a variable fee or credit based on volume, or may be purely variable and is common in IT outsourcing transactions.
- A fee based on the number of FTE resources used to perform the services. These charges are often based on FTE hourly, daily or monthly rates. This approach often is used in business process outsourcing (BPO) and application development outsourcings where there are productivity commitments to help manage the resources. Increasingly, in automation and technology-enabled BPO arrangements, the technology components that drive automation and the related systems integration, development and support may be priced separately.
- A fee based on the supplier's costs, commonly referred to as a cost-plus model. This method requires the supplier to disclose its costs, which makes this method rare.
- A fee based on the number of users or transactions. As the number of users or transactions fluctuates, the fees fluctuate. This method is more common in BPO arrangements.

Certain distinct parts of outsourcing arrangements, such as the transition, may be priced on a fixed-fee or FTE basis, which may be tied to the completion of certain milestones.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

These transfers are much less common in today's market, with the prevailing trend being to extend usage of the subject of the third-party contracts without actually transferring the contract. However, if relevant, the transfer should be in writing, addressed in the contract, and noticed or documented as required under the applicable third-party contract. These transfers may require consents from third parties, may be governed by an agreement with such third parties, and may be subject to certain charges.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Services may be subject to state and local sales and use taxes, typically depending on the states from which the services are provided and received. If assets are transferred (e.g., software, equipment, facilities, real estate), the transfer may be subject to federal, state and/or local taxes. Outsourcing transactions that include a cloud- or other internet-based service delivery component may also trigger taxation of services provided over the internet, with taxation occurring at various points of receipt of the services and apportionment required based upon the extent of use from state to state. The contract typically allocates financial and remittance responsibility for taxes in connection with the arrangement. The customer is often responsible for applicable sales and use taxes, with remittance by the supplier, except in unusual circumstances. Each party retains responsibility for the taxes on their income and on their assets.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Issues vary depending on the parties, available leverage and the operational purpose of the software. The following are a handful of key issues that a customer/licensee should consider:

- Authorised Users – Who are the appropriate users of, or are otherwise permitted to access, the software (e.g., affiliates of the licensee, end users, third-party hosting and/or service providers, customers, bots and automation tools, etc.)?
- Scope of Use – What are the permitted uses of the software by the licensee (e.g., are there business limitations, internal use limitation, quantity of transactions, revenue thresholds, etc.)?
- Implementation – Who is responsible for the implementation of the software? If the licensor will configure and implement the software, appropriate professional services need to be defined with additional relevant governing contract terms (e.g., acceptance and warranty provisions related to the professional services).
- Warranties/Warranty Remedies – What is the scope and duration of the software warranty, and what are the performance requirements measured against (e.g., documentation)? Also, what specific remedies are available to the licensee if the software fails to meet the warranty.
- Infringement – What is the licensor's responsibility, and what are the licensee's remedies if there is claim of infringement (e.g., indemnification, repair and replace, third-party licence, refund)?
- Limitation of Liability – What is the extent of the liability of the licensor if the licensor fails to implement the software, the software fails to perform, or there are infringement claims related to the software?

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Issues vary depending on the parties, available leverage and the operational purpose of the software. The following are a handful of key issues that a customer/licensee should consider:

- Scope of Support – How will the licensor provide the support and what access do they need to the licensee's environment? Are there any service level commitments regarding response and resolution times?
- Data Access – Will the supplier need access to the licensee's data (e.g., personal/regulated data)? Are there ways to limit access or otherwise obfuscate or protect this data? If personal data access is anticipated, appropriate data processing terms must be applied to cover processing requirements under applicable laws and regulations.
- New Versions/Releases – What are the licensor's commitments regarding the provision of new versions and releases

of the software? What obligation does the customer have to remain current and in what timeframe?

- Pricing – What are the licensor's commitments regarding future pricing? What is the maintenance and support term, including renewal options (consider the ROI period for the software licence)?
- Out of Support Options – What happens if the licensor no longer offers support? Is support available from a third-party supplier? Can the customer terminate support? If so, can the customer continue usage without support? Is there a right to reinstate support, and what is the cost to reinstate?

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Software escrow arrangements are more often used with niche providers and start-ups whose ongoing support capabilities or general viability are uncertain and for software that is particularly critical to operations. In today's market, escrow options exist for both premises-based licences and cloud subscriptions.

The enforceability of a software escrow agreement may be impacted by U.S. bankruptcy laws. However, there are provisions in the bankruptcy code that can be leveraged to permit the licensee to continue using the software and access the escrowed code in the event of licensor bankruptcy. The provisions in the escrow arrangement must be specifically drafted to take advantage of the bankruptcy provisions (including a present grant of a licence to the escrow materials).

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No, however, as noted herein, there are federal and state laws and regulations that impact and relate to the specific uses of cloud computing services in certain industries or applications (e.g., financial services, healthcare, the public sector and higher education).

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

The use of cloud computing solutions is almost ubiquitous in the U.S., with some pegging enterprise adoption at over 94% and with the market expected to grow by almost 28% in 2022.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The cloud deployment model has created a fairly standardised (provider-friendly) contracting framework in the U.S. The issues that are most negotiated are outlined in question 8.1 above with the following nuances being more customary:

- Warranties/Warranty Remedies – A warranty that the service will perform materially or substantially in accordance with the specifications or documentation, a warranty that changes to the cloud services and governing policies and terms will not materially and adversely affect the security, functionality or performance of the cloud services and a right for the customer to terminate the cloud services and receive a refund of prepaid fees in the event of a breach of the foregoing warranties that remains uncured (usually for 30 days or more).
- Data Privacy/Security – A commitment that the cloud provider will adhere to defined security standards and data processing terms and allocation of risk (exclusions from the limitations of liability and sometimes additional indemnities) for any breach of those standards or terms that causes or enables a compromise of personal data. Usually, liability in this context is limited to a separate, higher cap with types of damages being specified/limited to notification costs, fines, penalties and interest, and other remedial measures that companies customarily undertake to remediate the incident and restore their reputation in the event of a data breach.
- Disengagement/Data Migration – Whether, upon expiration or termination, the customer will simply have the right to download its data or, alternatively, to continue using the services for some period. The latter is the more common approach for operationally critical platforms. The format in which the customer data will be made available upon exit is often negotiated, with customers pushing for data to be made available in a format that is useable with commercially available software.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No, however, as noted herein, there are federal and state laws and regulations that impact and relate to the specific uses of AI solutions in certain industries or applications (e.g., financial services, healthcare, the public sector and higher education).

In addition, concerns over the misuse or unintended consequences of AI, and the benefits and consequences of its use, have prompted state legislatures to study the impact of AI on their constituents, with laws being enacted in four states in 2021. Many of these state laws and their resultant regulations focus on the study and impact of AI, while others are directed at preventing, or at least outlawing, the use and implementation of AI with discriminatory impacts.

At the federal level, recent examples include:

- Several federal agencies are implementing or considering new guidance relative to the use of AI, including the data sets used to train AI, in order to mitigate and address discriminatory outcomes and other adverse consequences. For example, in September 2021, the Department of Health and Human Services released the Trustworthy AI Playbook to provide guidance for the implementation of Trustworthy AI, and it is anticipated that the federal financial services regulatory agencies may release multi-agency guidance on the usage of AI in the financial services sector in 2022, following their 2021 request for information on AI pertaining to usage, governance, risk management and controls, and challenges in developing, adopting and managing AI.
- The Algorithmic Accountability Act of 2022 (pending as of June 1, 2022), which is intended to develop more public trust in AI, will require companies to take into account the impact of AI and automation and provide more transparency to consumers about the usage of AI and automation.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

The data used to train machine learning-based systems may be subject to certain data privacy laws and regulations (e.g., HIPAA, CCPA) and/or require consents from the data subject. In addition, depending on the sources of the data, the data may be protected by copyright laws. Accordingly, the ability to use (copy) copyrighted data to train machine learning-based systems without infringing the copyright of the underlying data, is a relevant, fact-based question that must be considered. The use of copyrighted data may be permissible under "fair use" standards, but that determination generally depends and turns on the purpose of the training of the machine learning-based systems (e.g., functional training, creating other copyrightable work, or creating a competing work). By contrast, publicly available data may have few, if any, restrictions. The aggregation of various data elements from multiple sources may also result in a compilation under copyright law and is also subject to further ownership by the copyright holder. A user of a machine learning-based system needs to identify each source of training data and ensure that it has the appropriate rights to use such data for the intended purpose, which may be obtained by licence and/or consent.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

The contract is likely to allocate ownership rights in any algorithms developed or improved as part of the machine learning techniques. Otherwise, the ownership of the IP rights in any algorithm that is improved without human involvement will be determined by applicable law, and ownership is likely to remain with the developer/creator of the original algorithm, although there is always some uncertainty with governing law allocations, especially in this context where the laws have not caught up with the changes in technology in this area.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, but several states have enacted laws that pertain specifically to the usage of blockchain, many of which enable the use of blockchain for corporate records (e.g., corporate ledgers), smart contracts, signatures and in legal proceedings and to permit the trade of corporate stocks on a blockchain. Cryptocurrencies that leverage blockchain technology are subject to numerous federal and state laws and regulations, which are a function of the financial services nature of the currency and not the usage of blockchain technology itself.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain is most widely adopted in the financial services sector. However, cross-industry adoption for supply chain use cases is significant, and use cases in the healthcare sector are prevalent. In addition, the use of non-fungible tokens (NFTs) is expanding in the entertainment, professional sports and other arenas. For example, in connection with the 2022 Draft, the National Football League is launching a series of card-themed NFTs, and several luxury fashion brands are expanding into monetizing branded digital assets using NFTs.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

In many respects, the issues are common to those outlined in section 8 for licensed solutions, those outlined in section 9 for cloud-based solutions, and those outlined in section 7 and this chapter generally for related development, systems integration and support services. However, there are some unique considerations for blockchain:

- Multi-Jurisdictional Issues – The distributed nature of many blockchain solutions require consideration of:
  - Jurisdiction-specific data privacy compliance obligations.
  - An effective means of dispute resolution where the participants may reside in different jurisdictions and an appropriate governing law that will yield a predictable outcome should disputes arise (see section 3).
- Exit and Data Return/Destruction – The distributed and immutable nature of blockchain technology itself requires careful consideration of a participant's ability to seek return or destruction of its data upon exiting the arrangement. If the user does not hold a copy of the ledger, then provisions must be negotiated for provision of data where required. If the blockchain is truly immutable, traditional return/destruction may have to be foregone in favour of encryption or other means of rendering the data inaccessible.
- Intellectual Property – Ownership of the blockchain technology itself and improvements to the technology, as well as allocation of ownership of the data on the blockchain should be dealt with contractually.
- Accountability/Liability – In a shared blockchain solution, the participants should contractually allocate responsibility for not only operation and support of the blockchain, but also for issues and liability that may arise in connection with usage of the blockchain (e.g., defects, data privacy/security, etc.).

Sean Christy co-leads BCLP's Technology and Commercial Transactions Group and is a trusted business and legal advisor to BCLP's clients in strategic technology and commercial transactions, including traditional and digital outsourcing transactions; strategic IT software, products and service arrangements (including IoT, AI, ML, and data sharing arrangements); cloud and other XaaS arrangements; technology-driven or dependent M&A; and other strategic commercial transactions. The scope of his work ranges from global transactions by multinational corporations to the core business deals of early-stage start-up companies. Sean's role as a business and commercial advisor to his clients is often a critical component in his clients' success.

Bryan Cave Leighton Paisner LLP
One Atlantic Center 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
USA

Tel: +1 404 572 6754
Email: sean.christy@bclplaw.com
URL: www.bclplaw.com

Chuck Hollis co-leads BCLP's Technology and Commercial Transactions Group. Chuck is a proven business and legal advisor to his clients, not only providing transactional legal advice, but also negotiation business strategy, vendor selection and consultative advice. His broad technology and commercial transactions experience includes global support across a variety of industries for the purchase, sale and implementation of cloud services, broad scale implementation of ERP, SaaS, XaaS, AI/ML and other technology and software platforms, and also includes support for the more traditional outsourcing arrangements (ITO, BPO, ADM) and strategic commercial transactions. In many cases, these arrangements are associated with corporate transactions, carveouts, joint ventures and divestitures.

Bryan Cave Leighton Paisner LLP
One Atlantic Center 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
USA

Tel: +1 404 572 6751
Email: chuck.hollis@bclplaw.com
URL: www.bclplaw.com

Derek Johnston has over 25 years of experience representing public and privately-held companies in complex business process outsourcing (BPO) and information technology outsourcing (ITO) transactions, strategic IT products and service engagements, software licensing, maintenance and development agreements, including software as a service (SaaS) and cloud computing arrangements, internet-related and other technology-based service agreements, and other strategic procurements. His work in these areas has focused on Fortune 1000 clients in the financial services, hospitality, restaurant, franchise, consumer products, electronics, utility, energy and online data/analytics industries.

Bryan Cave Leighton Paisner LLP
One Atlantic Center 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
USA

Tel: +1 404 572 6752
Email: derek.johnston@bclplaw.com
URL: www.bclplaw.com

Anne Friedman focuses her practice on structuring and negotiating large scale strategic sourcing and technology transactions, concentrating on global and domestic outsourcings in the areas of information technology, software development and maintenance, and business process outsourcing. Her practice also includes drafting and negotiating transition services agreements in connection with M&A transactions, software licensing, integration and implementation transactions, hosting agreements, distribution agreements, related corporate transactions, and handling issues relating to data privacy, data security and intellectual property matters.

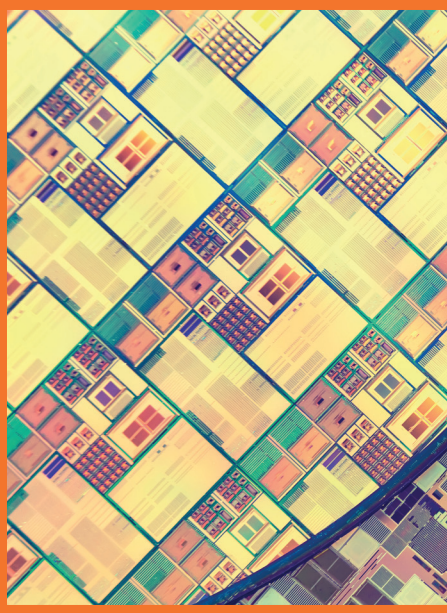
Bryan Cave Leighton Paisner LLP
120 Broadway, Suite 300
Santa Monica, CA 90401-2386
USA

Tel: +1 310 576 2209
Email: anne.friedman@bclplaw.com
URL: www.bclplaw.com

With over 1,200 lawyers in 30 offices across North America, Europe, the Middle East and Asia, Bryan Cave Leighton Paisner LLP is a fully integrated global law firm that provides clients with connected legal advice, wherever and whenever they need it. The firm is known for its relationship-driven, collaborative culture, diverse legal experience and industry-shaping innovation and offers clients a globally ranked technology and commercial transactions practice that assists clients with the full spectrum of technology sourcing matters covered by this chapter.

www.bclplaw.com

ICLG.com



Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group