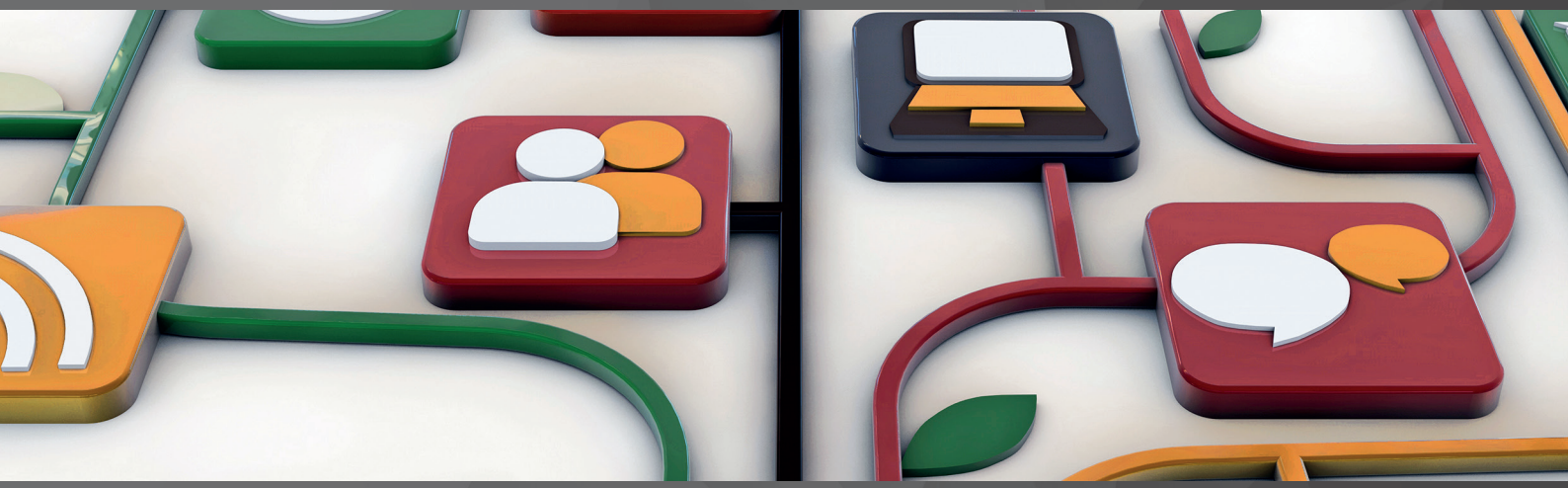
International
Comparative
Legal Guides



# Technology Sourcing 2021

A practical cross-border insight into technology sourcing

**First Edition**

**Featuring contributions from:**

Arioli Law

ASBZ Advogados

Astrea

Bird & Bird

Bryan Cave Leighton Paisner LLP

BSN Bufete Sánchez Navarro, S.C.

Cliffe Dekker Hofmeyr Inc.

Dana Associés

Fieldfisher

Goodmans LLP

Gorriceta Africa Cauton & Saavedra

Ikeyi Shittu & Co.

SHUSAKU·YAMAMOTO

TMT Law Practice

Wistrand Law Firm

ICLG.com

# Expert Analysis Chapter



# Q&A Chapters

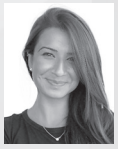
# Canada



Richard Corley


Jessica Bishop


Peter Ruby


Ida Mahmoudi

Goodmans 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?**

There are no federal or provincial Canadian laws that regulate the procurement of all technology products and services. However, certain aspects of the procurement of technology products and services are subject to certain required and/or guidelines (as detailed below), and a number of technologies are subject to specific regulation.

**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?**

Public sector bodies at the federal, provincial and, in some cases, municipal levels must comply with applicable public procurement requirements. The Canadian Free Trade Agreement (CFTA), and the growing list of international trade agreements that Canada is party to, impose principles of fairness, transparency and non-discrimination on an increasingly broad spectrum of public procurements. Further, if the technology products and services involve the collection, use, retention or disclosure of personal information collected by or for, or in the possession of, a public sector body, federal and/or provincial privacy regulations may apply.

## 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 minimum or maximum terms are imposed by Canadian law.

**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?**

Canadian law does not. However, in exceptional circumstances equitable principles could apply to require a reasonable notice period (e.g., if an outsourcing arrangement were to involve a significant imbalance of power and a high level of dependency of one party on the other).

**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?**

There is a limited common law duty to act in good faith in the performance of contractual obligations. In 2014, in *Bhasin v. Hrynew,* [2014] 3 SCR 494, the Supreme Court of Canada ruled that good faith is a general organising principle and that contractual duties must be performed honestly. Contracting parties may include provisions attempting to minimise the scope of good faith obligations, however courts are unlikely to enforce such provisions.

In 2021, the decision in *Wastech Services Ltd. v. Greater Vancouver Sewerage and Drainage District*, [2021] SCC 7 provided clarity on the duty to exercise contractual discretion in good faith. *Wastech* holds that contracting parties have a duty to exercise contractual discretion in good faith. This duty requires parties to exercise their contractual discretion in a manner consistent with the purposes for which it was granted under the contract.

In Québec, Articles 6 and 7 of the Civil Code of Québec codify a duty of good faith, which extends to the negotiation and performance of contracts.

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

Contract law generally provides that a customer can recover damages in the event that the terms of a technology-related solutions or services contract are breached. Failure on the part of the supplier to perform obligations under the agreement can result in other remedies such as injunctive relief, equitable remedies, or specific performance. Limitations on the types and amounts of damages are typically negotiated in most technology-related solutions or services contracts in Canada.

**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?**

In addition to service level fee reductions (discussed below) and the typical representations, warranties, covenants and indemnities, remedial provisions in technology-related solutions or services agreements are wide ranging and may include:

performance bonds; guarantees from the supplier's parent and/or affiliates; the ability to hold back or reduce fees; rights of set-off, step-in rights; access to supplier intellectual property (IP); and a wide variety of termination rights empowering the customer to terminate the agreement for breach or for convenience.

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

There are several avenues by which parties may terminate an agreement early. The most straightforward method to terminate an agreement arises when both parties agree to terminate the contract at a specified time.

A party may also terminate an agreement for convenience, but it is more common for this option to be available to the customer unilaterally. While terminating an agreement for convenience will not give rise to damages, termination for convenience often imposes notice and payment obligations on the terminating party.

Other grounds for terminating an agreement may include for a change in control, frustration of a contract, failure to achieve a milestone, and an event of *force majeure*.

**2.7 Can the parties exclude or agree additional termination rights?**

The parties are generally free to exclude or include any additional termination rights (providing such rights are consistent with public policy). Additional termination rights often include termination upon a material breach that is not cured during a specified period, less serious recurring breaches, repeated service level breaches, insolvency or a change of control of the supplier.

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

Parties are generally free to limit and exclude liability, unless the exclusion is interpreted as being unconscionable (being manifestly unfair) or violating public policy, such as excluding liability for fraud. It is common for limitations and exclusions of liability to be heavily negotiated. The supplier typically seeks to limit or exclude their liability for indirect, consequential, incidental and special damages, including any loss of business, profit or revenue where the loss constitutes a direct loss. Conversely, the customer seeks to ensure it can recover all direct losses. If the outsourcing arrangement is one where the supplier has access to the customer's confidential information, the customer typically seeks to have the supplier be fully liable for all damages relating to any breach of the confidentiality obligations.

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

Parties are free, and it is common practice, to include a financial cap (or caps) on liability, typically subject to a number of exceptions. The financial cap (or caps), and exceptions, in each outsourcing agreement depend on a variety of factors, including the nature of the services, the term of the agreement, the relative bargaining power of the parties, and prevailing industry practice.

**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?**

None of the general principles vary; however, certain aspects of the procurement of various types of technology products and services may be subject to industry or sector specific differences.

## 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?**

When entering into an agreement for the procurement of technology solutions and services, customers and suppliers typically will agree to a progressive approach to dispute resolution. The first stage usually involves escalating communications to designated parties for each of the customer and supplier with a goal of resolving the dispute. The second stage is often non-binding mediation, followed by either arbitration or litigation.

The level of detail included in the dispute resolution provision will depend on the sophistication of the parties, as well as the subject matter of the agreement. The parties may, for example, wish to identify a roster of arbitrators, who have a particular expertise. The parties may also exclude certain areas from binding arbitration. For example, disputes arising from IP infringement may be excluded from the dispute resolution process so that the injured party is able to seek relief from the courts.

## 4 Intellectual Property Rights

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

Intellectual property rights in Canada are typically protected by statutory intellectual property laws (consistent with international treaties), and express contractual provisions. Technology sourcing agreements usually include express provisions allocating ownership and licence rights in the intellectual property developed and used under such agreements.

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

In instances where intellectual property is being transferred, transfers must be in writing and in some cases should be registered with the Canadian Intellectual Property Office. The rules for ownership of IP depend on the type of IP. It is critical to document IP ownership clauses in agreements with employees, contractors and suppliers that assign the applicable IP to the assignee in each case. It also is necessary in Canada to have a waiver of moral rights signed by each person involved in the creation of work protected by copyright. Key concepts to cover in an agreement that involves an assignment and/or licensing

of IP include each party's rights with respect to: background IP owned by each party before the agreement; and IP generated during the agreement.

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

Under Canadian common law, confidential information is protected through contractual obligations to keep such information secret and to use it only for the purposes agreed to by the parties. Confidential information can also be protected through trade secret and breach of confidence law.

## 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?

Technology services contracts must reflect and allocate responsibility for ensuring that the privacy obligations of the parties under applicable legislation are met. There may be a requirement to notify or seek the consent of the individual to whom the information relates, before the proposed collection, use or disclosure of their personal information. There may also be obligations on a party to take appropriate steps to ensure that the personal information is safeguarded by the other party and only used for the defined purposes.

In Canada, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and/or corresponding provincial privacy laws govern the collection, use and disclosure of personal information in the private sector. These laws apply to the collection, use and disclosure of personal information, regardless of the form of the information or technology used.

PIPEDA applies to federal works, undertakings and businesses, and to private sector organisations that collect, use or disclose personal information in the course of commercial activities in provinces that do not have substantially similar legislation (currently Alberta, British Columbia and Québec). In addition, certain provinces have specific health information privacy statutes that apply to the extent that personal health information is processed in the context of a technology services contract.

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

PIPEDA applies to all personal information that flows across provincial or national borders in the course of commercial transactions. Although PIPEDA and related provincial legislation do not prohibit the transfer of personal data outside of Canada, PIPEDA requires that a "comparable level of protection" be provided when personal information is being processed by a third party through "contractual or other means". As such, if an organisation transfers personal information to a third party, the transfer must be "reasonable" for the purposes for which the information was initially collected, the information must be protected using contractual means, and the organisation should be transparent about its information-handling practices, including notifying individuals with respect to the transfer. In addition, the Québec *Privacy Act* requires organisations to consider the potential risks involved in transferring personal information outside of Québec. If the information will not receive adequate protection, it must not be transferred. In addition, privacy regulators have held that notice of such transfers must be provided to affected individuals – along with notice that such personal information may be subject to access requests from foreign governments, courts, law enforcement officials and national security authorities, according to foreign laws.

With respect to the public sector, additional restrictions and formalities may apply. For instance, public sector privacy legislation in British Columbia and Nova Scotia imposes restrictions on public bodies (and suppliers that may process personal information on their behalf) with respect to transfers of personal information. Personal health information may also be subject to additional restrictions with respect to transfers of such information outside of the applicable province.

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

Personal information, in particular, sensitive health information and information that can facilitate identity theft, are protected under a variety of federal and provincial laws, as well as industry standards (such as the Payment Card Industries Data Security Standard).

## 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?

Whether employees are transferred by operation of law depends on a number of factors. The jurisdiction, the structure of the transaction and the employees' union status are all relevant to consider. For example, if an outsourcing transaction is structured as a transfer of shares, Canadian employment law does not recognise any change in employer. All employees, including any associated liabilities would be carried through to the supplier, uninterrupted. This is true regardless of union status or jurisdiction. However, in an asset purchase, whether such a transfer occurs will highly depend on the applicable jurisdiction. In most Canadian jurisdictions, non-unionised employees are not transferred by operation of law. Unionised employees may be transferred by operation of law if the transaction constitutes a "sale of business" under applicable labour legislation. In such instances, the union's collective bargaining rights could extend to the supplier. Even then, whether such employees are transferred to the supplier will depend on the specific terms of the applicable collective bargaining agreement (CBA).

If employees are transferred by operation of law, the terms of employment would remain as is, unless otherwise negotiated and agreed to as part of the outsourcing transaction.

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

As part of the due diligence phase, parties typically share basic employment information such as the number of employees and the material terms of the employment. They may also share employee information needed for benefit plan enrolment. Canadian privacy legislation may limit the sharing of certain personal information.

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

In a non-unionised setting, it is not unusual, in connection with an outsourcing transaction, that employees may be terminated (in accordance with applicable Canadian employment law). Unionised employees are subject to the terms of the applicable CBA. CBAs often protect unionised employees from termination, barring misconduct. However, CBAs may also explicitly contemplate a "changed business" environment and allow terminations in such instances.

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

For non-unionised employees, yes. Such harmonised terms would be made clear in the offer to the employees. If material changes were made without the employees' consent, a constructive dismissal or breach of contract could result, on which employees could base a claim for damages. Any changes to the terms of unionised employees' employment require union agreement.

### 6.5 Are there any pensions considerations?

Yes. The considerations will be driven by the nature of the benefits provided to the employees by the supplier and the jurisdiction of the plan. Pension benefits are regulated under federal tax legislation and the applicable pension benefits legislation. The applicable legislation is based on the province of registration of the pension plan, and the location of the affected employees. Consideration must be given to the fiduciary responsibilities of the employer to the plan and its members, and to any collectively bargained benefits. Further, expert advice is often required concerning dispositions and transfers of pension assets held in registered retirement plans. Considerations on portability, accrual of benefits and other pension administration will depend on the jurisdiction and the type of pension provided, such as a defined benefit or defined contribution pension plan, or other type of retirement benefit plan.

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

Privacy law, as discussed in more detail above, is a key consideration in offshore outsourcing transactions. It is extremely rare for employees in Canada to be re-located offshore in connection with an outsourcing transaction. In most cases employees not retained by the service provider in the same roles onshore are either moved to other positions within the business or have their employment terminated in accordance with applicable agreements and provincial or federal law.

## 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)?

Generally, there are no federal or provincial Canadian laws that specifically regulate outsourcing transactions. However, certain aspects of an outsourcing transaction may be subject to industry or sector specific regulations and/or guidelines. For example, the Office of the Superintendent of Financial Institutions (Canada) (OSFI) provides guidelines for certain federally regulated entities (e.g., banks, credit unions) entering into outsourcing agreements. In addition to the financial sector, the following is a non-exhaustive list of industry sectors that are subject to regulation in Canada, each of which may subject certain types of outsourcing transactions to additional regulatory requirements: telecommunications; broadcasting; education; energy; gambling/lottery; healthcare; transportation; and environment. In each case, the applicable requirements are industry specific. Additionally, the structure of an outsourcing transaction may be viewed by applicable regulatory bodies as mergers or acquisitions, which could subject the transaction to notification and/or review under the Competition Act and/or the Investment Canada Act.

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

The most common and straightforward legal structure is a direct outsourcing agreement under which the customer contracts directly with the supplier. The agreement is typically entered into by the customer's operating company and the supplier (or the supplier's local affiliate). This structure consists of one or more agreements that prescribe the services provided, the payment terms, key personnel and assets, and the supplier's performance obligations and the consequences of failing to meet those obligations. A provision may be included to permit affiliates of the customer to have work performed under the main agreement or to enter into separate agreements or statements of work that incorporate the terms of the main agreement.

In some cases, outsourcing agreements may be entered into as part of or in connection with mergers and acquisitions, joint venture arrangements or other corporate or commercial arrangements.

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

Service levels prescribe the levels of performance the supplier must meet, and the agreement must detail the consequences of failures to meet such service levels.

Service levels typically measure performance in terms of availability, reliability, responsiveness, accuracy and other similar criteria.

Service levels may take the form of performance objectives (service level objectives or SLOs) or contractual commitments (service level agreements or SLAs). Breaches of SLOs typically result in responses through governance, including potential requirements for root cause analysis, remedial action and executive escalation. Breaches of SLAs typically give rise to fee reductions, responses through governance, and other potential remedial measures such as termination for breach in the event of repeated, significant breaches of SLAs.

Service level fee reductions are typically calculated as a percentage of the fees paid for the services and are intended to better align the interests of the supplier with that of the customer. Such fee reductions are to reflect the reduction in the value of the services to the customer and are not considered a penalty.

In some cases, suppliers may have an opportunity to earn back a portion of the most recent service level fee reduction by successfully implementing changes that enable them to consistently meet expected service levels (substantially above the minimum service levels at which fee reductions apply).

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

The specific charging methods used in Canadian outsourcing agreements depend on the nature of the services provided. While some services or projects are performed on a fixed price basis, it is more common that the price of the service scales with the volume of the service (such as hours of labour, number of transactions, number of customers serviced, number of computers maintained, etc.). Pricing can also reflect gain-sharing, sharing of benefits and other incentive arrangements.

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

The terms of any third-party contracts should be reviewed to identify whether assignment is possible without notice to the counterparty or express consent. As with the transfer of any contract, parties should also consider whether the third-party contract should transfer to the supplier by novation. If the transferring party desires to fully extricate itself from liability for non-performance, it must obtain the consent of the non-transferring party to the contract (novation). In most novations, each party agrees that: (i) the transferee is substituted for the transferor party as a party to the contract; (ii) the transferor is no longer liable for performance under the contract; and (iii) the transferee is directly and solely liable for the transferor's performance under the contract.

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

Canadian withholding tax obligations may arise when payments are made to non-residents for services rendered in Canada. Additionally, foreign suppliers may be subject to withholding tax when carrying on business in Canada. In some instances, these taxes may be limited due to tax treaties between Canada and other countries. With a transfer of assets, sales or commodity taxes (and in some cases separate provincial sales taxes) will apply. Exemptions may apply to certain eligible transfers.

## 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)?

The customer must obtain licence rights that enable the required scope of use for the appropriate term (perpetual *versus* term licence). Any restrictions on the licence grant should be carefully considered to accurately reflect the customer's use case, including any restrictions on the number of authorised users. The customer should consider any required use of the licensed software by any affiliates, contractors, other suppliers, clients, users or third parties that the customer may rely on to maintain, access or use the licensed software. The licence rights should also allow for an appropriate number of copies to be made for production use, back-up and archival purposes, disaster recovery and any other anticipated business purposes that could arise during the licence term. If the licence is restricted by geography, processors or location, consider whether those restrictions are acceptable and allow for adequate flexibility in the event of a business expansion, assignment or change to the location of the server on which the licensed software is stored. Given the increasing shift to cloud-based servers, the customer may also want to consider including a right to move the licensed software to a third-party cloud. The software licensing agreement should also provide terms governing the necessary updates, patches and releases for the licensed software, as well as the provision of support and maintenance for the software. Other considerations include cost, scalability, accessibility, data protection, data location and security.

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

Generally, the key considerations for the customer relate to: rights related to new versions, releases, updates and bug fixes; the process that the vendor will follow with the customer for rolling out the foregoing new versions, releases, updates and bug fixes; any support required by the customer for non-current versions of the software; the obligations and timelines for handling of incidents related to the provision of support and maintenance by the vendor; and the support and maintenance fees.

The customer will want to ensure that the contract clearly states whether or not the customer is entitled to new versions of the software, releases, updates and bug fixes and that those concepts are well defined. If the customer requires the right to test and accept any new versions, releases or updates before such changes are made to the software, is important to ensure that the contract provides the right to do so and a process governing such changes to the software. This may be particularly important where the software is integrated with other customer software or systems and changes to the software could impact such integrations. The customer may also want the right to keep two or more versions of the software with an accompanying right to continued support and maintenance of any such non-current versions of the software.

The fees for support and maintenance of software are often charged separately and may be linked to the licence fee, or it may be included in the licence fee. Whether separate or included in the licence fee, the customer will want to confirm that the fees for support and maintenance are clear. To provide price certainty, the customer may also want to ensure that any allowable increases to the fees for the support and maintenance are capped or can only increase by a pre-determined amount during the initial term and possibly during any renewal terms, depending on the business arrangement.

### 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 commonly used to provide a software licensee with access to the source code of licensed software in circumstances under which the licensor is no longer able to maintain the software, and the licensee wishes to take over such responsibilities itself. A properly structured and implemented software escrow arrangement may be enforceable and

effective in the event of an insolvency. However, the licensee will want to take care to ensure, among other things, that: (i) the escrowed source code is either self-escrowed or held by a trusted third party under a clear and enforceable agreement with the licensee; (ii) the trigger for source code release is clear and appropriate, and does not require the consent or acknowledgment of the licensor; (iii) the escrowed source code is current, complete and fully documented (such that it may be compiled to make the current version of the object code); and (iv) the grant of the licence to modify and compile the source code is clear and effective and is not subject to attack as an executory contract under Canadian insolvency laws.

## 9 Cloud Computing Services

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

Canada has no laws or regulations specific to the procurement of cloud computing services. However, certain aspects of a cloud computing transaction may be subject to industry or sector specific regulations and/or guidelines. For example, OSFI provides guidelines for certain federally regulated entities (e.g., banks, credit unions) entering into technology agreements that apply to cloud computing services. For public sector customers, there may be additional restrictions related to the location of data and other issues.

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

The compelling economic advantages provided by cloud computing models have led to its increasingly rapid adoption by enterprise scale organisations as well as smaller and medium sized businesses. There are various models of cloud computing, primarily Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) that have been adopted in Canada. There are also various cloud deployment options commonly used, such as public clouds where servers are owned and operated by third-party suppliers, private clouds that typically consist of a dedicated data centre on a private network for an organisation (either on site or provided by a third-party provider), or hybrid clouds that combine the two deployment models that allow an organisation to move applications between public and private clouds.

These models and deployment alternatives afford organisations options to choose a model that best meets the risk profile of the type of service performed or data processed. Typically, the more high risk or critical business functions may be managed in a private cloud while the lower risk business functions may be managed in a public cloud or with a hybrid cloud.

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

Generally, the key issues to consider are: data security; location and segregation of data; privacy and regulatory considerations; service failure and business interruption; geographical risk; concentration risk (often associated with using one cloud supplier to host several key products or businesses); loss of control; and the use of subcontractors to provide services, including the flow down of key contract terms to the supplier's contract with such subcontractors.

## 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?**

Canada has no laws or regulations specific to the procurement of AI-based solutions or technologies. Currently, the relevant laws and regulations largely address the use of personal information, and PIPEDA (or similar provincial legislation) sets out the rules for how private sector organisations collect, use and disclose personal information about individuals.

It is important for organisations to carefully consider whether their AI-based solution will process personal information. As part of this consideration, organisations should generally consider the training data (if applicable), the data that will be processed by the AI-based solution, and the data output of the AI-based solution, which, in certain circumstances, can create new personal information.

As it relates to public sector procurement, the Government of Canada has issued its Directive on Automated Decision-Making that introduces rules that govern the use of any automated decision system developed or procured after April 1, 2020 within the Government of Canada. The Directive provides a risk-based framework that includes the provision of advance notice of automated decision-making and meaningful explanation of decisions.

**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?**

Canada has no laws or regulations that would specifically regulate the ownership or legal status of such data. In the absence of clear legislation or case law, it is critical that vendors and customers clearly allocate data use rights as between them in commercial contracts. The question of whether data can be licenced contractually would involve case-by-case consideration of the various specific facts, and questions such as the nature of the data, the rights that the party licensing the data has in the data, the terms of the contract and any laws or regulations that apply to the data, such as applicable privacy laws where personal information is part of the data.

**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?**

Canadian intellectual property legislation does not expressly contemplate the ownership of intellectual property in AI solutions that use machine learning algorithms. Generally, where an AI solution develops a work product, such as an algorithm, there is no "author" as this concept is currently understood in Canadian copyright law. Similarly, there is no "inventor", as this concept is currently understood in Canadian patent law. The underlying assumption is that a human would be the author, or inventor, and an AI solution was not contemplated as a creator when the statutory regime was developed. This question is the subject of active, ongoing discussions in Canada and globally.

## 11 Blockchain

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

Canada has no laws or regulations specific to the procurement of blockchain-based solutions. However, certain aspects of a cloud computing transaction may be subject to industry or sector specific regulations and/or guidelines. For example, OSFI provides guidelines for certain federally regulated entities (e.g., banks, credit unions) entering into technology agreements that apply to blockchain-based solutions. For public sector customers, there may be additional restrictions related to the location of data and other issues.

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

Currently, the industries that are most widely using blockchain-based technologies are: financial services and fintech (identity verification; digitisation of financial instruments; clearing and settlement functions; custody; loan syndication; insurance claims processing); payments (decentralised ledger for retail payments, cross-border payments and tokenised fiat, stablecoins and cryptocurrency); legal (smart contracts); and oil and gas transportation and supply-chain (virtual passports, monitoring good corporate governance). The various use cases and industries using blockchain-based technologies continue to evolve and change rapidly.

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

In addition to the usual technology risks, the use of blockchain raises additional legal concerns that highly depend on the nature of the blockchain-based technology as between public (or "permissionless") and private (or "permissioned") blockchains. For public blockchains, the key legal issues revolve around data protection and compliance with privacy and anti-money laundering legislation.

Distributed ledger technologies (DLTs) such as blockchain, in principle, create an immutable ledger with copies of the ledger distributed to each network participant, typically in various jurisdictions across the globe. In public DLT networks, the contents of the ledger can be viewed by anyone without restriction and can never be altered or removed. Generally, most records in a public DLT network will likely contain transaction information related to a token or coin, and therefore may be considered, in whole or in part, a financial transaction that may be subject to various regulatory obligations, including securities laws.

For the purposes of Canadian privacy laws, organisations should assume that public DLT networks contain personal information regardless of any additional information, beyond the base transaction information, for each record that is included in the applicable ledger. In a private blockchain, where participation must be approved, the technology can be designed to allow for compliance with privacy laws (privacy by design), anti-money laundering and other applicable laws and regulations. When procuring public or private blockchain-based technology, organisations should carefully assess whether Canadian privacy laws or securities laws apply to their activities, and with respect to privacy laws more specifically, whether they are collecting, using or disclosing personal information in the course of the activities.

**Richard Corley** is a partner at Goodmans and leads the firm's Outsourcing and Cleantech practice groups. Richard has over 25 years of experience advising clients on complex outsourcing transactions, technology, M&A, joint ventures, cleantech and technology-related matters. Richard is acknowledged as one of Canada's leading experts in the areas of IT and outsourcing and he has led the procurement, negotiation, implementation, renegotiation and resolution of disputes in many of Canada's most complex outsourcing transactions. He pioneered the use of standardised tools and real time issue resolution to facilitate the efficient preparation and management of outsourcing agreements based on well-developed precedents. He is a frequent speaker at professional conferences and seminars on outsourcing, technology and cleantech-related topics.

**Goodmans LLP**
333 Bay Street, Suite 3400
Toronto
Canada

Tel: +1 416 597 4197
Email: rcorley@goodmans.ca
URL: www.goodmans.ca

**Jessica Bishop** is a senior associate in a business law group at Goodmans. Her practice focuses on corporate and commercial law with a focus on complex commercial technology transactions. Jessica represents financial institutions, insurance companies, technology service providers, pension funds, government agencies and companies in the asset management, healthcare, energy, securities, and other sectors that are involved in the development, acquisition and use of technology. Jessica has extensive experience advising clients on technology procurement, outsourcing, cloud computing, payment systems, licensing, fintech, digital and e-commerce solutions, software development and systems implementation, data processing and privacy compliance.

**Goodmans LLP**
333 Bay Street, Suite 3400
Toronto
Canada

Tel: +1 416 597 4242
Email: jbishop@goodmans.ca
URL: www.goodmans.ca

**Peter Ruby** is a partner at Goodmans. He has a national and international practice focused on business and IT-based dispute resolution, including software, telecommunications, film, artificial intelligence, quantum computing, television, privacy/data protection and breach, IP, e-commerce/internet litigation, arbitration, mediation and advice. Peter represents multi-national and entrepreneurial vendors of technology and services, along with many end-users of information technology. He is also an arbitrator and mediator with Arbitration Place and ICDR. Peter is recognised as a leading IT litigator in *Chambers Global*, *The Canadian Legal Lexpert Directory*, *Euromoney's Guide to The World's Leading Information Technology Lawyers* and *The Best Lawyers in Canada*.

**Goodmans LLP**
333 Bay Street, Suite 3400
Toronto
Canada

Tel: +1 416 597 4184
Email: pruby@goodmans.ca
URL: www.goodmans.ca

**Ida Mahmoudi** is an associate in a business law group at Goodmans. She is developing her practice in the areas of mergers and acquisitions, securities law, corporate law, banking and finance law and technology law. Before joining Goodmans, Ida graduated *cum laude* from the University of Ottawa with a Specialization in Law and Technology. She was selected to research AI technologies with the Canada Research Chair in Ethics, Law, and Technology for three years and helped advise key government and technology bodies, including the Royal Canadian Navy, Transport Canada, the Department of National Defence and two Standing Committees at Parliament and Senate levels regarding various privacy and technology matters.

**Goodmans LLP**
333 Bay Street, Suite 3400
Toronto
Canada

Tel: +1 416 597 4217
Email: imahmoudi@goodmans.ca
URL: www.goodmans.ca

Goodmans LLP is recognised as one of Canada's pre-eminent business law firms, offering market leading expertise in M&A, corporate and transaction finance, private equity, REITs and income securities, outsourcing, real estate, tax, restructuring, litigation and other business-related specialties.
The firm represents a broad range of Canadian and foreign clients, from entrepreneurial businesses to multinational corporations, financial institutions, private equity firms, pension funds and governments and has a reputation for handling challenging problems, often international in scope, that demand creative solutions.
Our lawyers are consistently recognised by leading industry arbiters, and in various surveys of clients and peers conducted by *Lexpert*, *Lexpert/American Lawyer Media*, *Chambers and Partners*, *Euromoney*, *International Financial Law Review*, *Law Business Research*, *Best Lawyers in Canada* and *The Legal 500 Canada*.

**www.goodmans.ca**

Goodmans LLP

# ICLG.com

## Other 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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group