AI in Canada

A legal guide to developing and using artificial intelligence

September 10, 2025

OSLER

Table of contents

Introduction

Artificial Intelligence (AI) is transforming the world around us. What once seemed like science fiction, is increasingly becoming part of our daily lives. From generating answers to complex questions, to enhancing the provision of healthcare services, and everything in between, AI is profoundly altering how we work and live, while simultaneously creating unprecedented opportunities for innovation, improved productivity, and economic growth. Yet, with AI's transformative potential comes a host of complex legal and regulatory challenges that developers and users of AI tools must navigate carefully.

This guide is designed to provide a practical, business-oriented roadmap for organizations and individuals involved in the development, deployment, and use of AI systems. It addresses the multifaceted legal and operational issues that arise in the AI ecosystem, offering insights and actionable strategies to mitigate risk, enable compliance, and foster trust in AI technologies. By focusing on real-world applications and specific contexts — such as employment, healthcare, capital markets, legal services, and the public sector — this guide aims to equip developers and users of AI with the knowledge and tools necessary to make informed decisions in a rapidly evolving technological landscape.

Key issues addressed in the guide

This guide explores a broad spectrum of issues that are critical to the responsible development and use of AI, including:

- AI regulation and standards: Understanding emerging regulatory frameworks, industry standards, and best practices to ensure compliance and foster accountability.
- Copyright: Addressing questions around ownership of AI-generated works and the use of publicly available data for training models.
- Privacy: Navigating privacy laws, with a focus on the legal basis for collecting and using personal information, data minimization and privacy impact assessments.
- Human rights considerations: Ensuring that AI systems protect against bias and discrimination, and promote transparency and accountability.
- Tort liability and risk management: Assessing liability risks associated with AI errors, failures, and harms, as well as implementing strategies to mitigate exposure.
- Antitrust and competition law: Evaluating the competitive impacts of AI technologies, including concerns about price-fixing, collusion, and other anti-competitive practices.
- Commercial contracting: Drafting contracts that address AI-specific issues, such as intellectual property rights, regulatory compliance, and risk allocation.

Context-specific guidance

As the challenges and opportunities presented by AI vary across industries and sectors, this guide seeks to provide tailored insights for key areas of application:

- Employment: Managing the use of AI in hiring, performance evaluation, and workplace monitoring.
- Healthcare: Leveraging AI for the delivery of healthcare as well as for the development and deployment of medical devices.
- Capital markets: Harnessing AI for algorithmic trading and risk assessment.
- Legal services: Deploying AI to enhance the delivery of legal services, while addressing professional responsibility, privilege and confidentiality concerns.
- Public sector: Implementing AI in the delivery of government services, including through the deployment of automated decision making.

A practical, forward-looking approach

This guide is not merely a theoretical exploration of AI-related issues. Rather, it is a practical tool designed to help organizations and individuals navigate the complexities of AI development and use. Whether you are a developer of AI systems, in-house counsel, or a leader seeking to integrate AI into your operations, this guide provides a plethora of insights to help you tackle AI's various legal and regulatory challenges, while unlocking AI's full potential.

Overview of AI in Canada

Things to know

- Canada has long been at the forefront of AI advancements and recognized as a global leader in the field. Groundbreaking work in Canada by Geoffrey Hinton, Yoshua Bengio, and Yann LeCun — the "founding fathers of AI" — has laid the foundation for many modern AI innovations, including artificial neural networks, deep learning and reinforcement learning. Canada continues to rank highly in global AI research, consistently placing fourth in the Global AI Index.
- The Pan-Canadian Artificial Intelligence Strategy and the Canadian Sovereign AI Compute Strategy, introduced in 2024, underscores Canada's commitment to fostering domestic AI innovation and development. The launch of the Canadian AI Safety Institute, also in 2024, has reinforced Canada's commitment to the safe development and deployment of AI.
- While Canada's ambitions to foster a world-leading AI ecosystem create significant opportunities, understanding Canadian norms, standards and regulatory frameworks is critical when developing, distributing or deploying AI systems in Canada.

Things to do

- Develop a high-level understanding of AI within the Canadian landscape.
- Evaluate both the opportunities and risks associated with engaging in the Canadian AI market, including challenges related to data privacy, intellectual property protection, discrimination and product liability.
- Create a governance plan for meeting emerging regulatory standards for responsible AI and ensuring compliance with Canadian legal requirements for the procurement, adoption, development and deployment of AI.
- Collaborate with Canadian legal and industry experts to navigate jurisdiction-specific considerations to achieve your organizational objectives.

Useful resources

- "Pan-Canadian Artificial Intelligence Strategy," Innovation, Science and Economic Development Canada, December 2024
- "Canadian Sovereign AI Compute Strategy," Innovation, Science and Economic Development Canada, May 2025
- "Canada launches Canadian Artificial Intelligence Safety Institute," Innovation, Science and Economic Development Canada, November 12, 2024
- "Osler AI Series: A primer on the technology, common and emerging uses, opportunities and challenges," webinar hosted by Osler, March 7, 2023

Regulation of AI in Canada

Things to know

- There is no law in Canada that sets out a general framework for regulating AI models and systems. The bill that included Canada's proposed *Artificial Intelligence and Data Act* (AIDA) died on the Order Paper when Parliament was prorogued on January 6, 2025.
- The Department of Innovation, Science and Economic Development has published a voluntary code of conduct applicable to generative AI systems that have advanced capabilities enabling them to be adapted for a wide variety of uses in different contexts. Developers and managers of advanced generative systems that become signatories to the code make commitments in respect of accountability, safety, fairness and equity, transparency, human oversight and monitoring, and validity and robustness.
- There are multiple laws of general application that govern specific elements of the development and use of AI models and systems. Relevant laws include:
  - federal and provincial privacy laws which regulate the collection, use and disclosure of personal information in the context of the training of AI models and the generation of output. Privacy laws in Quebec include additional rules applicable to automated decision systems
  - copyright law which is relevant to the generation of training datasets, the training of AI models, and the generation of model output
  - federal and provincial human rights laws which prohibit discrimination on enumerated grounds (including race, colour and gender) in specific contexts (including employment and the provision of goods, services, facilities and accommodation)
  - tort laws (and similar provisions in Quebec's Civil Code) which hold organizations or individuals liable for damages caused through their negligence, including for products that they create or deploy. Other potentially relevant torts include defamation, misrepresentation, intentional infliction of mental distress, placing a person in a false light, and non-consensual distribution of intimate images
  - competition law which govern agreements, conduct and transactions that may prevent or lessen competition, and has been identified as a key area of focus given AI's potential to facilitate anti-competitive practices, such as collusion and deceptive marketing
  - employment laws, which regulate the use of AI in employment contexts such as hiring, monitoring, performance evaluation and termination
- Sector-specific requirements applicable to the use of AI models and systems also exist, including in connection with:
  - financial services (e.g., guidelines of the Office of the Superintendent of Financial Institutions that govern the use of models)
  - capital markets (e.g., Staff Notice and Consultation of the Canadian Securities

Administrators on how securities legislation applies to the use of AI)

- transportation (e.g., regulations applicable to the testing and use of autonomous vehicles on public roadways)
- legal services (e.g., guidelines issued by provincial law societies applicable to the use of generative AI by lawyers)
- public sector entities (e.g., guide for federal institutions on the use of generative AI)

Things to do

- Identify all existing laws and regulator guidance that may apply to your development or use of AI models or systems.
- Monitor legislative developments at the federal, provincial and municipal levels of government to identify regulatory requirements that may apply to your activities.
- Monitor guidelines, directives and decisions of regulators for rules governing the development or use of AI models or systems.
- Consider if, or to what extent, laws of other jurisdictions (such as the E.U.'s *Artificial Intelligence Act*) may apply to your AI-related activities.

Useful resources

- "Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems," Innovation, Science and Economic Development Canada, September 2023
- "Ethical Design and Use of Artificial Intelligence by Small and Medium Organizations," Digital Governance Council, CAN/DGSI 101:2025
- "Artificial intelligence and competition – Discussion Paper," Competition Bureau of Canada, March 2024
- "Consultation on Artificial Intelligence and Competition: What We Heard," Competition Bureau of Canada, January 27, 2025

AI standards

Things to know

- In the absence of legislative guidance, standards are critically important to guide the responsible development, deployment and use of AI.
- Standards setting organizations are rapidly developing a variety of standards applicable to AI. The most prominent include:
  - ISO/IEC 42001 – Information technology — Artificial intelligence — Management system, the first international standard for AI management systems.
    - ISO 42001 provides a series of controls for embedding responsible AI practices across an organization.
  - ISO/IEC 23894 – Information technology — Artificial intelligence — Guidance on risk management, an international standard for managing AI risk.
    - ISO 23894 – Information technology — Artificial intelligence — Guidance on risk management — supports lifecycle-based risk assessments and risk communication strategies.
  - NIST AI RMF 1.0 [PDF] – Artificial Intelligence Risk Management Framework, a standard published by the U.S. National Institute of Standards and Technology (NIST) is framework for managing risks across the AI lifecycle.
    - The NIST AI RMF Playbook describes action for achieving outcomes outlined in the Risk Management Framework.
- The Government of Canada's Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, introduced in October 2023 and expanded in 2025, encourages organizations to commit to key principles such as safety, transparency, accountability, fairness, and human oversight.
  - The Voluntary Code of Conduct distinguishes between organizations that develop advanced generative AI systems and those that manage or deploy them, with different expectations and commitments for each.
  - In March 2025, the federal government published the Guide for Managers of AI Systems, offering a useful practical tool for implementing the Voluntary Code.

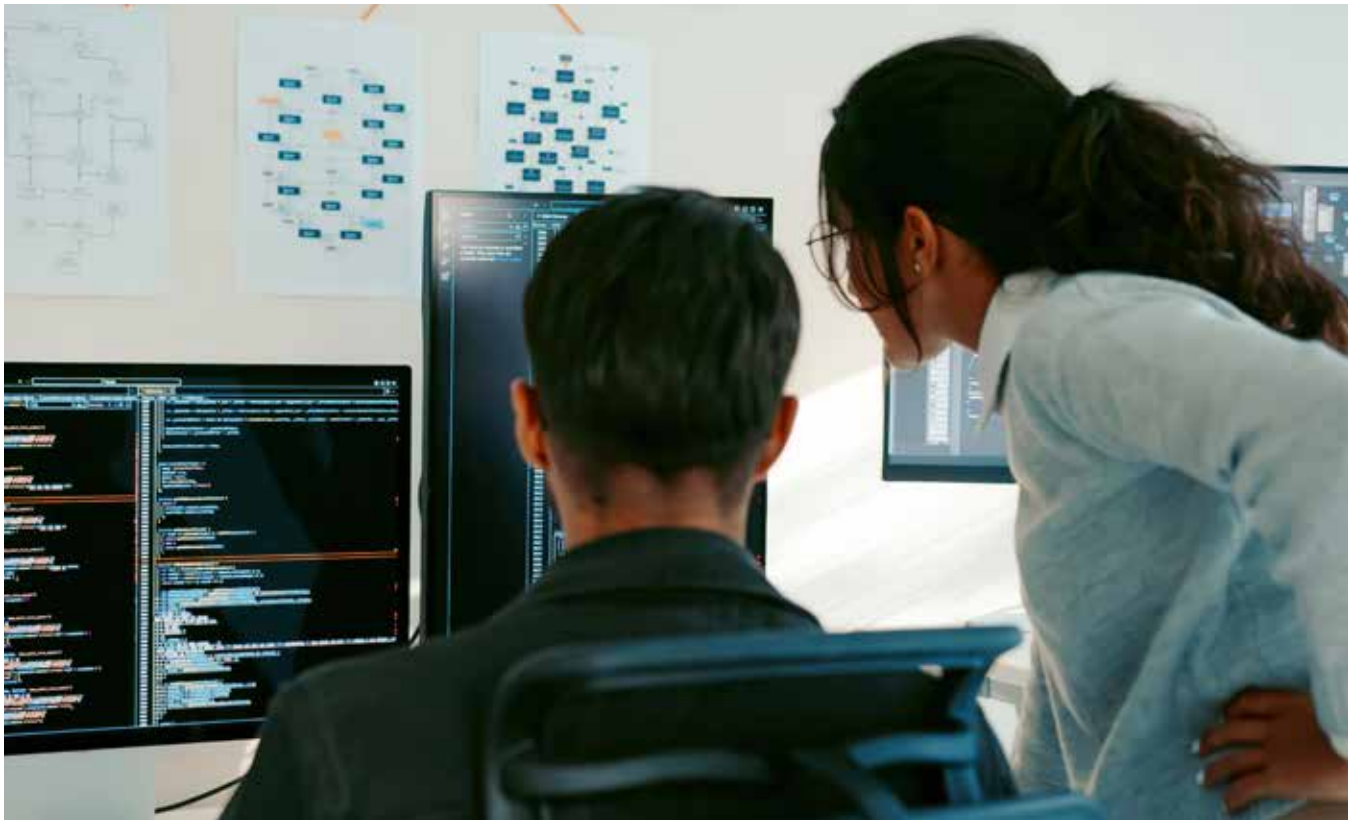
Things to do

- Understand the content of the standards and which parts of the standards apply to your particular development and use of AI.
- Consider the role that compliance with leading international AI standards can play in policy making and contracting for effective and responsible AI development and deployment.

- When contracting and procuring AI tools, consider utilizing these standards to create obligations around the effectiveness and responsible deployment of AI.
- Consider whether it is to your advantage to follow, adopt or sign on to the Government of Canada's Voluntary Code of Conduct on AI.
- Build flexibility into policies, contracts and procurement requirements to take into account evolving standards.

Useful resources

- International standards:
  - ISO/IEC 42001 – AI Management System
  - ISO/IEC 23894 – AI Risk Management
  - NIST AI Risk Management Framework (AI RMF 1.0)
- Canadian frameworks and guidance:
  - Ethical Design and Use of Artificial Intelligence by Small and Medium Organizations, CIO Strategy Council, CAN/DGSI 101:2025
  - Voluntary Code of Conduct for Generative AI
  - Guide for Managers of AI Systems (2025)
- Commentary and guidance:
  - "The role of ISO/IEC 42001 in AI governance," Osler, July 10, 2024



Application and compliance with foreign laws

Things to know

- AI is increasingly regulated across jurisdictions. Cross-border compliance is critical for companies operating globally, especially where AI systems may be classified differently (e.g., "high-risk" in the E.U. but not in Canada).
- The E.U.'s *Artificial Intelligence Act* is the world's first comprehensive AI regulation. It introduces a risk-based framework. Some AI systems and practices are prohibited, specific rules apply to identified "high-risk" AI systems and general purpose AI models, and transparency requirements apply to certain AI systems considered to be low risk. The rules are being phased in between February 2025 and August 2026. On July 10, 2025, the European Commission published The General-Purpose Code of Practice, a voluntary tool to assist developers of general purpose AI models to comply with the Act.
- U.S. AI policy remains fragmented. While some sector-specific rules exists, there is no broadly applicable federal AI law. While some state laws have been enacted, Congress is considering the enactment of a 10-year moratorium on state-level AI legislation.
- Canada has been an active participant in various international initiatives in respect of AI, including the creation of standards emphasizing human rights, accountability, and interoperability. These initiatives include:
  - the OECD's Recommendation of the Council on Artificial Intelligence (which sets out the first intergovernmental standard addressing AI, which is to be used by members to shape policies and create an AI risk framework across jurisdictions)
  - the UNESCO Recommendation on the Ethics of Artificial Intelligence (which addresses ethical issues)
- Canada is a founding signatory of the Council of Europe Framework Convention on AI, the first legally binding international treaty on AI, focused on human rights, democracy, and the rule of law.

Things to do

- Identify where your AI systems are developed, deployed, or sold, and determine if you are subject to foreign regulatory regimes such as the E.U. AI Act, U.S. sectoral laws, or treaty-based obligations.
- Consider AI procurement standards and model clauses when contracting with third-party AI developers or vendors and consider referencing model procurement standards (e.g., E.U. model clauses) to mitigate legal, operational, and reputational risks.

- Assess AI system classification under applicable foreign AI regulations:
  - Determine if your system falls under "prohibited," "high-risk," or "limited-risk" categories pursuant to the E.U.'s AI Act.
  - Prepare to implement technical documentation, conformity assessments, and human oversight for high-risk systems.
- Consider aligning your AI practices with international standards to demonstrate proactive governance and reduce compliance friction across jurisdictions.
- Implement internal compliance programs that integrate international standards (such as ISO/IEC 42001 and NIST AI RMF) to create a globally compatible AI governance framework.
- Monitor international developments in AI regulation and coordinate legal strategies across jurisdictions.

Useful resources

- National and international legal frameworks:
  - EU Artificial Intelligence Act, European Union, in force 2024
  - "The General-Purpose AI Code of Practice," European Commission, July 2025
  - "Model Artificial Intelligence Governance Framework: Second Edition [PDF]," Personal Data Protection Commission Singapore, Singapore, 2020
  - The Basic Act on the Development of Artificial Intelligence and the Establishment of Trust, South Korea, in force 2026
  - Interim Measures for the Management of Generative Artificial Intelligence Services, China, 2023
- Multilateral and treaty-based initiatives:
  - Council of Europe Framework Convention on AI [PDF]
  - "Recommendation of the Council on Artificial Intelligence," Organisation for Economic Co-operation and Development, 2024
  - "Recommendation on the Ethics of Artificial Intelligence," UNESCO, 2021
  - "Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI," Office of the Privacy Commissioner of Canada, October 2024

Copyright

Things to know

- Canadian copyright law does not provide specific rules for AI systems, but existing principles — especially relating to authorship, reproduction and fair dealing — are relevant when AI tools are developed, trained, and deployed.
- Authorship and ownership of AI-generated works is an open legal question in Canada. The default rule is that the author is the first owner of copyright (subject to certain exceptions). There is no definition of "author" in Canada's *Copyright Act*, but copyright jurisprudence suggests that an author must be a natural person.
- Text and data mining (TDM) exemptions are not expressly identified within the *Copyright Act*. While TDM may arguably be justified under a fair dealing exception to infringement, the legal status of TDM activities, including the reproduction of works to create datasets for training models, is unsettled.
- Fair dealing provides a potential defense for certain uses of copyrighted material by AI developers. Canadian courts have not ruled, however, on whether large-scale AI training constitutes "research" within the meaning of the exception. The fair dealing exception applies only to certain enumerated purposes, including research, private study, criticism, review and news reporting. To qualify, the dealing must also be "fair" based on a multi-factor analysis.

Things to do

- If you are training a machine learning model, evaluate whether the source material is protected by copyright and whether your use could be covered under the fair dealing exception. When possible, seek licenses or use public domain/openly licensed data.
- If you are deploying an AI model, be aware that output may infringe third-party rights if the model reproduces substantial parts of training data.
- If you are fine-tuning an AI model, assess copyright compliance in light of the new datasets and outputs, particularly where fine-tuning may lead to memorization or output similarity.
- If you are deploying an AI system, anticipate requirements to make copyright-related representations and warranties in commercial contracts. Representations may include that your system does not infringe third-party rights and that appropriate permissions or licenses are obtained.

Useful resources

- "Consultation on Copyright in the Age of Generative Artificial Intelligence," Innovation, Science and Economic Development Canada, 2023
- "Why AI could mean more work, not less, for copyright lawyers," Law Times, March 12, 2025
- "Time to talk about ownership of AI-generated intellectual property assets," Osler, December 13, 2021

Privacy considerations when developing AI

Things to know

- Canadian privacy laws apply to the development of AI if personal information is processed, for example, if personal information is used to train an AI model, if an AI model or system processes personal information, or if an AI model or system generates output that includes personal information.
- "Personal information" is broadly defined under Canadian privacy laws and includes information that can be used alone or in combination with other information to identify an individual.
- Unlike under privacy laws in some jurisdictions, such as the European Union, Canadian privacy laws are consent-based with limited exceptions to consent and do not include a "legitimate interests" legal basis for processing personal information.
- Publicly available personal information is subject to consent and other obligations under privacy laws with limited exceptions.
- It is uncertain whether or to what extent "implied consent" may be relied upon as legal authority for collecting or using personal information to train an AI model or generate output, or whether consent to use personal information to train an AI model or generate output can be made a "condition of service" (with no ability to opt out).

Things to do

- Identify and document your legal authority (i.e., consent or an exception to consent) for collecting and using personal information to train an AI model or generate output. When relying on consent, ensure that the consent is valid and meaningful. When sourcing personal information from a third party, obtain assurances that the information was collected lawfully and the third party has authority to disclose it to you for the intended purposes (e.g., AI model training).
- Remember that, with limited exceptions, publicly available personal information, including information published online, is subject to privacy laws in Canada (including when subject to an exception to consent).
- Be open and transparent (e.g., in your publicly-posted privacy policy and user flows) about what, how, when and why personal information is collected, used or disclosed during development, training or operation of the AI model or system, and provide this information in an understandable manner. Disclose any known limitations about the accuracy of AI outputs (e.g., age of data used to train the model) and any known or likely risks.

- Collect, use and disclose personal information only for documented, legitimate and appropriate purposes.
  - Do not use personal information to develop or deploy AI systems for purposes that violate "no-go zones" identified by the Office of the Privacy Commissioner of Canada, such as "*profiling that may lead to unfair, unethical or discriminatory treatment, or creating outputs that threaten fundamental rights and freedoms.*"
  - Use an adversarial testing process to identify potential unintended inappropriate uses of your AI model or system and, if applicable, take steps (such as technical measures or mandatory acceptable use policies) to prevent inappropriate uses.
- Collect, use, retain and disclose personal information only to the extent needed to fulfill the explicitly specified, appropriate purpose, including by removing personal information from datasets used to train AI models where possible and appropriate. Ensure that personal information used to train an AI model is accurate as necessary for the purpose of the model.
  - Do not use personal information when using anonymized or synthetic data will allow you to achieve your identified purpose.
  - When personal information is required, remove direct identifiers from the dataset wherever possible such that only de-identified personal information remains.
- Perform (and update over time) privacy impact assessments, algorithmic impact assessments and bias testing and assess resilience to inferencing or other attacks.
- Develop a comprehensive AI governance program and/or review and enhance your privacy governance program and security policies and practices to address AI-related issues, including by enabling individuals to request access to their personal information, ask questions, submit complaints and correct inaccurate personal information.
- Consider if, or to what extent, laws of other jurisdictions (such as the E.U.'s *Artificial Intelligence Act* or General Data Protection Regulation) apply to an AI model or system that you make available to users outside Canada.

Useful resources

- "Principles for responsible, trustworthy and privacy-protective generative AI technologies," Joint publication of the Office of the Privacy Commissioner of Canada and provincial data privacy regulators, December 7, 2023
- "Concluding joint statement on data scraping and the protection of privacy," Joint publication of the Office of the Privacy Commissioner of Canada and international data privacy regulators, October 2024

Privacy considerations when using AI

Things to know

- Canadian privacy laws apply if personal information is used to fine-tune an AI model, if a prompt entered into an AI model or system includes personal information, or if an AI model or system is used to generate output that includes personal information.
- "Personal information" is broadly defined under Canadian privacy law and includes information that can be used alone or in combination with other information to identify an individual.
- Unlike under privacy laws in some jurisdictions, such as the European Union, Canadian privacy laws are consent-based with limited exceptions to consent and do not include a "legitimate interests" legal basis for processing personal information.
- Compliance obligations vary depending on the nature of the organization and the industry in which it operates (e.g., financial services, telecommunications, retail, health or public sector), the nature and sensitivity of the personal information that is processed, and the activities the organization undertakes using an AI model or system (e.g., automated decision-making to grant a loan or select a job applicant).

Things to do

- Identify and document your legal authority (i.e., consent or an exception to consent) for collecting and using personal information to fine-tune an AI model or to prompt an AI model or system to generate output. When relying on consent, ensure that the consent is valid and meaningful. When sourcing personal information from a third party, obtain assurances that the information was collected lawfully and the third party has authority to disclose it to you for the intended purposes.
- Remember that publicly available personal information, including information published online, is subject to privacy laws in Canada (including when subject to an exception to consent).
- Be open and transparent (e.g., in your publicly-posted privacy policy and user flows) with individuals about what, how, when and why personal information is collected, used or disclosed during fine-tuning or use of an AI model or system, and provide this information in an understandable manner. Disclose any known limitations about the accuracy of AI outputs (e.g., age of data used to train the model) and any known or likely risks.

- Collect, use and disclose personal information only for documented, legitimate and appropriate purposes.
  - Avoid inappropriate uses of AI models or systems, including uses that violate "no-go zones" identified by Canadian privacy regulators, such as "profiling or categorization that may lead to unfair, unethical or discriminatory treatment that is contrary to human rights law; the collection, use, or disclosure of personal information for purposes that are known or likely to cause significant harm to individuals or groups, or activities which are known or likely to threaten fundamental rights and freedoms."
- Consider whether the use of an AI model or system that involves the collection, use or disclosure of personal information is necessary and proportionate and whether there are more privacy protective technologies that can be used to achieve the same purpose.
- Avoid prompting an AI model or system to re-identify data that has been previously de-identified.
- Consider whether the output of an AI model or system is accurate and reliable in the context of the intended purpose.
- Collect, use, retain and disclose personal information only to the extent needed to fulfill the explicitly specified, appropriate purpose.
  - Do not use personal information when anonymized or synthetic data will work for your purposes.
  - Where personal information is required, remove direct identifiers (e.g., from the prompts or output) wherever possible, such that only de-identified personal information remains.
- Ensure that personal information used to fine-tune an AI model is accurate as necessary for the purpose of the model.
- Perform (and update over time) privacy impact assessments, algorithmic impact assessments and bias testing and assess resilience to inferencing or other attacks.
- Develop a comprehensive AI governance program and/or review and enhance your privacy governance program and security policies and practices to address AI-related issues. This includes enabling individuals to request access to their personal information, ask questions, submit complaints and correct inaccurate personal information.
- For public-facing AI tools, ensure individuals know they are interacting with an AI tool and inform individuals of the privacy risks and options available to them.
- When using an AI system as part of a decision-making process:
  - clearly communicate to affected individuals the use of the system to make a decision, the general functioning of the system and how the system is used
  - clearly communicate, or be ready to communicate, to affected individuals how a decision that may have a significant impact on them was reached (including the personal information that was used to reach that decision), how to request a human review or reconsideration of the decision, how to request a correction of the personal information used, and any other recourse options
  - where appropriate, including where a decision will have a significant impact on the individual, include a human reviewer in the decision-making process

  - maintain adequate records to allow for requests by an affected individual for access to information about a decision
  - ensure decisions that relate to a specific group are made only after determining that the group is adequately and accurately represented in the system's training data
- Consider if, or to what extent, laws of general application (such as human rights laws and employment laws) apply to use of your AI model or system.
- Consider if, or to what extent, laws of other jurisdictions (such as the E.U.'s *Artificial Intelligence Act* or General Data Protection Regulation) apply to the use of your AI model or system.

Useful resources

- "Principles for responsible, trustworthy and privacy-protective generative AI technologies," Joint publication of the Office of the Privacy Commissioner of Canada and provincial data privacy regulators, December 7, 2023

Human rights

Things to know

- If safeguards are not in place to protect against bias and discrimination, AI systems could result in, or perpetuate, human rights violations which, in addition to creating liability, could erode trust amongst affected individuals.
- Human rights are protected under applicable human rights legislation. In Ontario, the governing legislation is the *Human Rights Code*, R.S.O. 1990, c. H.19 (the OHRC). The OHRC specifically focuses on protecting individuals from discrimination in aspects of public life such as employment, housing and services.
- Canada is a signatory to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. The Convention aims to ensure that AI systems are consistent with human rights, democracy and the rule of law without stifling technological progress and innovation. The Convention will come into force once five states, including at least three Council of Europe Member States, agree to be legally bound by it.
- The Law Commission of Ontario and the Ontario Human Rights Commission have published a Human Rights AI Impact Assessment tool. The tool provides a framework for organizations to assess their AI models and systems to ensure they comply with human rights legislation.
- Organizations are responsible for the outputs generated by the AI models and systems they use. In general, it may be difficult for users of models and systems to shift liability for breaches of human rights legislation to the providers of the model or system.

Things to do

- Consider if, or to what extent, an AI model or system may present compliance or litigation risks under Canadian human rights laws, including in relation to hiring, performance management and employment termination issues.
- Ensure human rights law and policy is considered in the design and/or implementation of AI models and systems.
- Understand the terms of use governing an AI tool that relate to the treatment of data inputted into the tool as well as any contractual or statutory obligations owed to third parties that might impact the use of the tool.
- Develop policies and procedures to test for bias throughout the life cycle of an AI model or system as well as strategies for mitigating bias should it be detected.
- Ensure all applicable stakeholders within your organization, such as human resources, legal teams and information technology departments, have a seat at the table to identify risks and risk mitigation strategies.

- Ensure AI models and systems are not "black boxes" (so that you are able to explain why a decision was made, including by pointing to objective and non-discriminatory reasons).
- Ensure that privacy, confidentiality and privilege considerations are addressed before using third party impact assessment or similar tools.

Useful resources

- "Human Rights AI Impact Assessment [PDF]," The Law Commission of Ontario and the Ontario Human Rights Commission, November 2024
- "Human Rights AI Impact Assessment Backgrounder [PDF]," The Law Commission of Ontario, March 2025
- "Directive on Automated Decision-Making," The Government of Canada, June 24, 2025
- "The Framework Convention on Artificial Intelligence," Council of Europe

Tort liability

Things to know

- Canadian tort law does not specifically address AI models or systems, but existing legal principles — particularly negligence and those that generally apply to product liability claims — apply where a model or system causes a third party to be harmed.
- Additional torts such as defamation, misrepresentation, intentional infliction of mental distress, intrusion upon seclusion, breach of confidentiality, placing a person in a false light, and non-consensual distribution of intimate images (among others) may be relevant, particularly in the context of chatbots, generative AI content generation, predictive AI, and deep fakes.

Things to do

- Conduct regular risk assessments of AI models or systems to monitor system performance and identify foreseeable harms to users and third parties. Ensure risk assessments take into account how a model or system may be used and the potential for malfunction or misuse.
- Establish robust governance, human oversight and quality assurance measures, especially where AI is deployed in high-risk or safety-sensitive sectors.
- Assess risks associated with how any applied AI makes use of proprietary or confidential data and, in particular, whether there are potential risks arising from the data sources and/or the transmission of proprietary data outside of the enterprise (including to foreign jurisdictions).
- Document the design, testing, and deployment processes to support defence of claims made by third parties.
- Monitor legal developments and prevailing industry standards and prepare to adapt your AI model or system use practices to align with applicable legal requirements and industry guidance.
- Explore what AI-insurance is available to protect against claims resulting from AI models or systems not functioning as expected.

Useful resources

- "Report on Artificial Intelligence and Civil Liability [PDF]," British Columbia Law Institute, April 2024
- "Addressing the Liability Gap in AI Accidents [PDF]," Centre for International Governance Innovation, July 2023
- "Chatbots: who could be liable for the accuracy of the output?", Osler, March 1, 2024

Competition and foreign investment laws

Things to know

- The *Canadian Competition Act* applies to agreements, arrangements, transactions, and other conduct that may prevent or lessen competition and to false or misleading representations to the public.
- AI has been a key recent area of focus for the Competition Bureau, which enforces the *Competition Act* and completed a detailed *Consultation on Artificial Intelligence and Competition* in January 2025.
  - The consultation concluded that the complexity of AI markets may distinguish them from other digital markets and discussed how the use of AI can have both positive and negative impacts on competition.
  - On the positive side, AI may lead to improved product quality, greater pricing options, and expanded product offerings, which may be relevant factors when a transaction or other conduct is being reviewed by the Competition Bureau. AI may also lead to efficient and pro-competitive outcomes by enabling companies to maintain a consistent pricing approach aligned with their goals as markets shift.
  - On the negative side, AI may facilitate anti-competitive conduct, such as collusion between competitors and deceptive marketing practices.
- Under the *Competition Act*, it is a criminal offense for competitors, or potential competitors, to enter into agreements or arrangements to fix prices or wages; allocate markets, territories, or customers; control production or supply; or engage in bid rigging. This can be proven from circumstantial evidence alone, such as the sharing of competitively sensitive information between competitors.
- A single AI system or algorithm could facilitate a "hub-and-spoke" conspiracy as the central hub used by multiple competitors to coordinate on pricing, with alleged conduct of this nature leading to investigations in both Canada and the U.S.
- The *Competition Act* also prohibits making false or misleading representations to the public for the purpose of promoting products, services, or business interests. AI could be used to amplify deceptive marketing practices by generating fake online reviews, endorsements, impersonations, or tailored phishing campaigns.

Foreign investment

- Investments by non-Canadians to establish new Canadian businesses or acquire control over an existing Canadian business are either notifiable or reviewable under the *Investment Canada Act*.

- All investments by non-Canadians in Canada, regardless of size or structure, can be reviewed on a discretionary basis on national security grounds. National security reviews can result in orders blocking an investment, authorizing it on certain terms and conditions, or requiring divestitures.
- AI technology has been identified as an area of potential sensitivity in guidance on national security reviews under the *Investment Canada Act*.

Things to do

- Ensure that the unique features of AI markets are taken into account when assessing the potential risks of a transaction being reviewed by the Competition Bureau.
- Exercise caution before using an AI model or third-party algorithm to inform pricing or other competitive strategies to avoid violating criminal prohibitions against price fixing and other collusive behaviour among competitors.
- Avoid sharing competitively sensitive information with an AI model or third-party algorithm, which could raise risks of potential criminal violations of competition laws. Examples of sensitive information include pricing, bidding strategies, supply/output levels, employee wages, and customer/supplier information.
- Never use AI to generate fake online reviews, endorsements, impersonations, tailored phishing campaigns, or other potential deceptive marketing practices.

Foreign investment

- Before buying, selling, or establishing a Canadian business that develops or utilizes AI technology, assess the potential risk of a national security review under the *Investment Canada Act*.
- Proactively prepare to address and respond to potential national security questions or concerns when buying, selling, or establishing a Canadian business that develops or utilizes AI technology.

Useful resources

- "Consultation on Artificial Intelligence and Competition: What We Heard," Competition Bureau of Canada, January 2025
- "Artificial Intelligence and Competition: Discussion Paper," Competition Bureau of Canada, March 2024
- "Guidelines on the National Security Review of Investments," Government of Canada, Revised March 2025
- "Sensitive Technology List," National security and defence, February 2025
- Frequently asked questions concerning the Investment Canada Act, Innovation, Science, and Economic Development Canada, September 2023

Employment considerations

Things to know

- AI is being increasingly leveraged in the context of hiring and managing employees, giving rise to concerns about bias, transparency, explainability, accuracy and fairness. Human rights legislation can be critically important in the employment context (see the "human rights considerations" section of this guide for more information).
- Most Canadian workplaces are governed by provincial legislation and regulations, while only a subset (e.g., airlines, banks and telecommunications companies) are regulated by federal legislation.
- Ontario's *Working for Workers Four Act, 2024*, S.O. 2024, c. 3 amended the *Employment Standards Act, 2000*, S.O. 2000, c. 41 to introduce a mandatory disclosure requirement for employers who use AI to screen, assess or select applicants for publicly advertised job postings. The disclosure requirement comes into force on January 1, 2026. "Artificial intelligence" is defined under the *Employment Standards Act* as:

  > "A machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments."

- Use of AI systems in the workplace, without appropriate safeguards, can lead to various employment-related risks such as claims of bias, discrimination and/or constructive dismissal.

Things to do

- Assess the use of AI in employment processes, paying particular attention to applications that implicate individuals, for example, where AI is used to screen, assess or select applicants for jobs.
- Manage potential risks associated with the use of AI tools in the workplace by developing AI governance and usage policies.
- Ensure human resources, legal and information technology professionals have a voice and clear role in AI governance, procurement, contracting and vendor negotiations to consider mitigation of employment law risks.
- Craft transparent and accurate disclosure statements for publicly advertised job postings in Ontario where AI is used to screen, assess or select applicants. Be prepared to answer inquiries from job candidates and existing employees with respect to how AI is used.
- Ensure employees receive appropriate guidance and training on the responsible use of AI tools in the workplace. For example, employers must advise their employees that certain information cannot be inputted into AI tools (i.e., confidential and/or personal information).

Useful resources

- "Resolution on Artificial Intelligence and Employment [PDF]," co-sponsored by the Office of the Privacy Commissioner, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner of Ontario, and the Office of IPC BC, October 2023
- "Artificial intelligence in the hiring process," The Government of Canada
- "Directive on Automated Decision-Making," The Government of Canada
- "Implications of Artificial Intelligence Technologies for the Canadian Labour Force [PDF]," House of Commons Canada
- "'Working for workers' means more work for employers," Osler, September 5, 2024
- "Working for Workers Four: 'artificial intelligence' disclosure requirement," Osler, December 17, 2024

Healthcare and medical devices

Things to know

Healthcare professionals:

- Canadian privacy laws and the policies and standards of health regulatory authorities apply to healthcare professionals using AI in their health practices.
- Healthcare professionals using AI are responsible for ensuring appropriate safeguards are in place to protect patient data and may be required to obtain express patient consent prior to using AI products in their healthcare practice.

Medical devices:

- Health Canada has issued guidance for manufacturers of machine learning-enabled medical devices (MLMDs) when demonstrating the safety and effectiveness of their MLMD as part of an MLMD licence application.
- The onus is on manufacturers of MLMDs applying to Health Canada for a medical device licence to declare the use of machine learning in their device and to classify their MLMD as a class II, III or IV medical device.
- Health Canada does not prescribe specific supporting information that must form a part of an MLMD application and will apply a risk-based approach to determine compliance with the evidence-based safety and effectiveness requirements.

Things to do

Health professionals who use AI:

- Understand the applicable legal and professional obligations relating to the privacy and confidentiality of patient data when using AI, how patient data will be transferred, stored and used and whether reasonable safeguards are in place to protect patient data.
- Be aware of the limitations of certain AI products, such as AI scribes, and review all information generated by AI for accuracy and completeness.
- Ensure patients are informed about how AI is used by the healthcare practice and obtain patient consent to use AI when necessary.

Manufacturers of MLMDs:

- Abide by "good machine learning practice" when designing, developing, evaluating, deploying and maintaining an MLMD.

- Use data to develop an MLMD that is representative of the Canadian population and clinical practice.
- Consider whether a predetermined change control plan will be included in the MLMD licence application to provide a mechanism for Health Canada to address cases where the regulatory pre-authorization of planned changes to machine learning systems is needed to address a known risk.
- Continue to observe the safety and effectiveness requirements applicable to MLMDs following the pre-market phase throughout the entire product lifecycle.
- Develop post-market monitoring plans and include in MLMD licence applications a description of the processes, surveillance and performance monitoring plans, and risk mitigation strategies to ensure ongoing performance.

Useful resources

- "Pre-market guidance for machine learning-enabled medical devices," Health Canada, February 2025
- "Good Machine Learning Practice for Medical Device Development: Guiding Principles," Health Canada, October 2021
- "AI Scribes: Answers to Frequently Asked Questions," Canadian Medical Protective Association, December 2023
- "AI Scribes in Clinical Practice," College of Physicians and Surgeons of Ontario, June 2024
- "Artificial Intelligence in Generated Patient Record Content [PDF]," College of Physicians and Surgeons of Alberta, September 2023
- "Considerations for adopting and implementing artificial intelligence (AI) in healthcare," Canadian Medical Protective Association, October 2024

Capital markets

Things to know

- In December 2024, the Canadian Securities Administrators (CSA) issued Staff Notice and Consultation 11-348 (the Staff Notice), clarifying how existing Canadian securities laws apply to the use of AI systems in capital markets.
  - The Staff Notice underscores the importance of deploying AI systems with a high degree of explainability to promote transparency and assist market participants with satisfying their obligations under securities law.
- Canadian financial institutions, fintechs, market participants, and issuers that utilize AI — either internally developed or through third-party providers — all face responsibility for ensuring their compliance with securities laws.
- Ontario Securities Commission priorities are to support an environment where:
  - the deployment of AI systems enhances the investor experience while the risk of investor harm is addressed
  - markets can benefit from potential efficiencies and increased competition brought on by the use of AI systems
  - regulatory clarity supports capital formation in this sector
  - any new types of risks, including systemic risks, are appropriately mitigated

Things to do

- Disclosure obligations: Identify and comply with disclosure obligations in respect of the use of AI, be transparent to investors and/or clients about how AI systems are used, any associated risks, and risk management activities, as highlighted by the Staff Notice.
- AI governance: Develop and implement comprehensive AI governance frameworks to guide AI system planning, design, verification and validation. AI governance policies should be aligned with the Staff Notice recommendations.
- Oversight mechanisms: Establish robust overnight mechanisms, in alignment with the Staff Notice recommendations which includes human-in-the-loop, AI literacy, and risk training.

Useful resources

- "CSA Staff Notice and Consultation 11-348 – Applicability of Canadian Securities Laws and the use of Artificial Intelligence Systems in Capital Markets," Ontario Securities Commission, December 2024
- "Navigating AI systems in capital markets: recent guidance from the CSA," Osler Risk Management and Crisis Response Blog, December 18, 2024
- "Artificial Intelligence in Capital Markets: exploring use cases in Ontario [PDF]," Ontario Securities Commission and Ernst & Young LLP

Using generative AI to provide legal services

Things to know

- Provincial and territorial law societies govern the conduct of lawyers and paralegals in Canada, including by providing guidance on legal and ethical issues.
- Most law societies have issued guidance that sets out guardrails and measures that licensees should implement when using generative AI in their legal practice. Common themes in the law society guidance include:
  - the need to understand generative AI in general and to conduct due diligence on the specific generative AI tools being used
  - the importance of being transparent with clients about the use of AI to perform legal services
  - the importance of maintaining the confidentiality of client information
  - the importance of maintaining privilege
  - the importance of independently verifying AI-generated content
- Given that many issues around AI and privilege are yet to be considered by Canadian courts, making privileged information accessible by any AI model should be approached with caution. Similarly, in interacting with AI for legal purposes, it should not be assumed that all prompts and output will be protected by privilege.

Things to do

- Understand the operational and legal risks and limitations of generative AI, including issues relating to client confidentiality, privilege, copyright infringement and ownership of AI content.
- Develop and maintain internal policies or guidelines on the use of generative AI. Among other topics, ensure that client confidentiality and privilege are addressed.
- Review AI-generated content to ensure it meets ethical and legal standards. Scrutinize results for biases. Verify through fact-checking that results are accurate.
- Do not include within prompts any confidential or sensitive information, or information that could otherwise be used to identify clients or specific legal matters, without first conducting thorough due diligence on the security of the AI tool and the use of inputs by the applicable provider.
- Check with the court, tribunal, or other relevant decision-maker about requirements for attributing the use of generative AI. By way of example, the Federal Court and various provincial courts require counsel to inform the court and other parties if any litigation documents contain AI-generated content. Certain courts separately now require counsel to certify as to the authenticity of all case law relied upon in written briefing.

- Review the relevant guidelines from law societies in the jurisdictions that you operate in to identify the specific requirements with which you will need to comply. By way of example, some law societies, including from the Barreau du Québec, provide specific guidance around record-keeping in respect of the use of generative AI tools.
- Consider if, or to what extent, laws of general application (such as privacy laws and human rights laws) apply to your use of generative AI tools.

Useful resources

- "L'intelligence artificielle générative: Guide pratique pour une utilisation responsable [PDF]," Barreau du Québec, October 25, 2024
- "The Generative AI Playbook: How Lawyers Can Safely Take Advantage of the Opportunities Offered by Generative AI," Law Society of Alberta, January 2024
- "Practice Resource: Guidance on Professional Responsibility and Generative AI [PDF]," Law Society of British Columbia, October 2023
- "White paper: Licensee use of generative artificial intelligence [PDF]," Law Society of Ontario, April 2024
- "Guidelines for the Use of Generative Artificial Intelligence in the Practice of Law [PDF]," Law Society of Saskatchewan, February 2024
- "Generative Artificial Intelligence: Guidelines for Use in the Practice of Law [PDF]," The Law Society of Manitoba, April 2024
- "Artificial Intelligence in the Practice of Law: What is AI and can I or should I use it in my practice? [PDF] Nova Scotia Barristers' Society, 2023
- "Guidelines for the Use of Generative AI in the Practice of Law," Law Society of the Northwest Territories, January 2025
- "Artificial Intelligence in Your Practice," The Law Society of Newfoundland & Labrador
- "Notice to the Parties and the Profession: The Use of Artificial Intelligence in Court Proceedings [PDF]," Federal Court, May 7, 2024
- "Practice Direction – Re: Use of Artificial Intelligence in Court Submissions [PDF]," Court of King's Bench of Manitoba, June 23, 2023
- "Ensuring the Integrity of Court Submissions when using Generative Artificial Intelligence ("AI") [PDF]," Supreme Court of Nova Scotia, October 18, 2023
- "Use of Artificial Intelligence (AI) and Protecting the Integrity of Court Submissions in Provincial Court [PDF]," Provincial Court of Nova Scotia, October 27, 2023
- "Notice to the Profession and General Public: Ensuring the Integrity of Court Submissions When Using Large Language Models [PDF]," Supreme Court of Newfoundland and Labrador, October 12, 2023
- "Practice Direction – General-29: Use of Artificial Intelligence Tools [PDF]," Supreme Court of Yukon, June 26, 2023

Public sector

Things to know

- The use of AI by federal public sector entities is addressed by Treasury Board of Canada Secretariat (TBS) policies, directives and guidelines; particularly, the Directive on Automated Decision-Making and related materials. This directive applies to all automated decision systems developed or procured after April 1, 2020, and is intended to ensure that systems used by federal institutions to support or make administrative decisions, including systems that rely on AI, are transparent, accountable, and legally compliant, promoting fairness and reducing risks to Canadians.
- The federal government has also issued guidance that advises federal institutions on responsibly using and developing generative AI tools, emphasizing cautious use, risk assessments, and limiting usage to scenarios where risks can be effectively managed.
- The provinces and territories are developing their own guidance use and procurement of AI. In Ontario, the *Strengthening Cyber Security and Building Trust in the Public Sector Act* enacted in November 2024, provides a legislative framework for governing the use of AI by public sector entities. Public sector entities may be required to publicly disclose specified information about their use of AI systems, develop and implement accountability frameworks applicable to such use, and take steps to manage related risk. The specific requirements governing the use of AI systems will be set out in future regulations.

Things to do

- Review the Directive on Automated Decision-Making to assess if it applies to you and, if so, identify the applicable compliance requirements. By way of example, the requirements may include completing a prescribed Algorithmic Impact Assessment (AIA) and meeting transparency, quality assurance and procedural fairness rules.
- When deciding whether to use generative AI tools:
  - identify and review any guidance or policies applicable to the use of AI within the public body or institution
  - consider experimenting with low-risk uses of generative AI, for example, editing a draft of a document that will undergo additional human review, before considering higher-risk uses like deploying a tool for use by the public
  - ensure that employees can access and participate in training on the effective and responsible use of the tools
- Before proposing to use generative AI tools:
  - assess and mitigate ethical, legal and other risks
  - determine whether a Privacy Impact Assessment is needed

- consult with key stakeholders (including legal counsel and privacy office) before deploying generative AI tools for use by the public and before using such tools for service delivery purposes
- implement risk management strategies to identify, assess and mitigate potential risks associated with AI systems
- update external policies/notices to provide information to the public about the use of AI systems
- review applicable privacy legislation and related policy instruments, which govern the handling of personal information by the public body, to identify requirements for when and how personal information is collected, created, used or disclosed using a generative AI system
- avoid inputting personal information into publicly available online generative AI tools
- be aware of integrity and security risks of using generative AI and consider the best practices recommended by the Canadian Centre for Cyber Security in their guidance Generative Artificial intelligence (AI) - ITSAP.00.041
- tailor risk-mitigation measures to each use
- consider aligning use of AI with the Treasury Board Secretariat's "FASTER" principles: Fair, Accountable, Secure, Transparent, Educated and Relevant.
- review applicable directives or policies (e.g., for federal public bodies, the Directive on Service and Digital) to identify requirements with respect to documenting activities and decisions related to the use of AI tools. By way of example, you may be required to keep records of decisions to develop or deploy generative AI tools and steps taken to ensure that outputs produced by the tools are accurate
- identify requirements in respect of the retention and disposal of documentation surrounding the use, development and deployment of generative AI systems under the control of a government institution

Useful resources

- "Directive on Automated Decision-Making," Government of Canada, June 24, 2025
- "Directive on Service and Digital," Government of Canada, January 10, 2024
- "Generative artificial intelligence (AI) - ITSAP.00.041," Canadian Centre for Cyber Security, July 2023
- "Guide on the use of generative artificial intelligence," Government of Canada, June 3, 2025
- "Strengthening Cyber Security and Building Trust in the Public Sector Act," Government of Ontario, assented to November 25, 2024

Contracting for AI applications

Things to know

- Given the nature of artificial intelligence, particularly large language models, most companies seeking to derive value from AI will procure — not build — AI systems. Effective contracting that takes into account the particularities of AI technologies is critical.
- Contracting frameworks for information technology generally are used as the basis for acquisition or sale of AI products and related services, but many unique attributes of AI products and services require that particular attention be applied to AI-specific issues.

Things to do

- Delineate the components of an AI system which may include foundational models, fine-tuned models, algorithms producing models, data, software applications and interfaces, and agents.
- Allocate rights to the various components of the AI system; this often requires going beyond a simple allocation based on products, existing or background intellectual property and ownership new works, to more complex discussions about grants of license rights, restrictions on use and other factors on the various components comprising the AI system.
- Account for compliance issues by allocating related responsibilities and including mechanisms to deal with changes arising from quickly developing regulatory requirements and standards.
- Address issues relating to data that are inherent in AI systems, such as data used to train models, use and disposition of customer data, query data, and outputs.
- Incorporate necessary elements of responsible AI into the contractual arrangement, including, as applicable, model accuracy testing and improvement, transparency, and bias testing.
- Include commitments on reliability and availability commensurate with the importance of the business function being enabled by the AI product or service.
- Allocate risk by way of warranties, indemnities and limitations of liability through a risk-based approach to creation, use and management of the AI system. Carefully account for the risks associated with the specific AI system distinguishing between the system itself and the outputs.

Useful resources

- "Navigating the legal landscape of AI commercial contracting," Osler, September 17, 2024

Key Contacts

Sam Ip
Partner, Technology

sip@osler.com
416.862.5955

Simon Hodgett
Partner, Technology

shodgett@osler.com
416.862.6819

Michael Fekete
Partner, Technology

mfekete@osler.com
416.862.6792

About Osler, Hoskin & Harcourt LLP

Osler is a leading law firm with a singular focus – your business. From Toronto, Montréal, Calgary, Vancouver, Ottawa and New York, we advise our Canadian, U.S. and international clients on an array of domestic and cross-border legal issues. Our collaborative "one firm" approach draws on the expertise of over 600 lawyers to provide responsive, proactive and practical legal solutions driven by your business needs. For more than 160 years, we've built a reputation for solving problems, removing obstacles, and providing the answers you need, when you need them.

Osler, Hoskin & Harcourt LLP
Toronto Montréal Calgary Vancouver Ottawa New York | **osler.com**

OSLER