大成 DENTONS

Part three of Canada's new federal privacy Bill C-27: *Artificial Intelligence and Data Act*

Introduction

We live in a time of significant growth of artificial intelligence (AI) technology, and we are bearing witness to ever more computers being built with algorithms that have the potential to automate decision making. We see this in new self-driving automobiles, medical diagnostic tools, drone technologies, legal research, language translation services and many more applications. Within this context, on June 16, 2022, the Canadian government tabled Bill C-27 *"An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,"* which includes the proposed *Artificial Intelligence and Data Act* (AIDA)[1].

AIDA builds upon the Canadian government's stated desire to encourage the responsible adoption of AI systems that are "human-centric and grounded in human rights, inclusion, diversity, innovation and economic growth"[2] by establishing Canada-wide requirements for the design, development, use and provision of AI systems.

Among other things, AIDA reflects the concerns many have with the potential for AI systems to do harm, both mentally and physically, to human beings. Additional concerns have been raised with respect to the significance of AI systems being programmed with biased algorithms, whether intentionally or unintentionally. Accordingly, AIDA specifically calls on persons responsible for certain AI systems to be cognizant of the potential for biased output and mitigate against those risks, and this proposed legislation has made it an offence to develop an AI system available for use when knowing or being reckless as to whether the use of an AI system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property.

This insight provides a summary of the key provisions of AIDA applicable to Canadian businesses, and discusses potential associated costs that may be incurred by these businesses to comply with its requirements. This insight also compares AIDA to other global initiatives regarding AI legislation and includes a comparison chart that highlights AIDA's fit within the global AI regulatory space.

A future insight will provide commentary on predominant themes that are emerging from global initiatives regarding AI and issues we can expect to encounter with respect to the application of AIDA if and when it comes into force.

Summary of the key provisions of AIDA

A. Key definitions in AIDA

- "**AI system**" means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning, or another technique in order to: (a) generate content; or (b) make decisions, recommendations or predictions.
- "**Biased output**" means content that is generated, or a decision, recommendation or prediction that is made, by an AI system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination as set out in section 3 of the *Canadian Human Rights Act*, or on a combination of such prohibited grounds. These prohibited grounds include (among others):
  a. Race;
  b. National or ethnic origin;
  c. Colour;
  d. Religion;
  e. Age;
  f. Sex; and
  g. Sexual orientation.

---

1 Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022) [*AIDA*].

2 Canada's Digital Charter in Action: A Plan by Canadians, for Canadians (2019), online: <https://ised-isde.canada.ca/site/innovation-better-canada/sites/default/files/attachments/Digitalcharter_Report_EN.pdf> at 21.

Notably, "**biased output**" does not include content, or a decision, recommendation, or prediction that has the purpose and effect of: (a) preventing disadvantages that are likely to be suffered by; or (b) eliminating or reducing disadvantages that are suffered by; any group of individuals when those disadvantages would be based on or related to the prohibited grounds of discrimination.

- "**Regulated activity**" means any of the following activities carried out in the course of international or interprovincial trade and commerce:
  a. Processing or making available for use any data relating to human activities for the purpose of designing, developing or using an AI system; and/or
  b. Designing, developing or making available for use an AI system or managing its operations.

B. Who is being regulated under AIDA?

Any person who carries out any regulated activity and who processes or makes available for use anonymized data in the course of that activity will be regulated under AIDA. A "person" includes a trust, a joint venture, a partnership, an unincorporated association and any other legal entity; however, AIDA does not apply to government institutions. The Government of Canada has addressed the issue of potential harms of the use of automated decision making by its institutions and their providers through the Treasury Board of Canada Directive on Automated Decision Making[3].

C. What is being regulated under AIDA?

The overarching purpose of AIDA is to regulate international and interprovincial trade and commerce in AI systems. Through AIDA, it is intended that common requirements will be implemented, applicable across Canada, for the design, development and use of AI systems. Furthermore, AIDA will prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or their interests.

Notably:

a. **Persons carrying out any regulated activity**: Persons carrying out any regulated activity and processing or making available for use anonymized data in the course of that activity will be required to establish measures with respect to how that data is anonymized and how that data is used and/or managed.
b. **Persons who are responsible for an AI system**: Persons responsible for an AI system will be obligated to assess whether it is a "high-impact system" and will be required to keep a record of the reasons supporting an assessment of a system as being a high-impact system. The regulations to AIDA will provide definition and guidance as to what constitutes a high-impact system, but draft regulations have not yet been released. Our expectation is that the scope and definition of what constitutes a high-impact system will be similar to how both the European Commission's "White Paper on Artificial Intelligence" and the European Union's *Artificial Intelligence Act,* discussed below, define and frame what constitutes a "high-risk" AI application or system.

   Similar to the foregoing, persons responsible for a high-impact system will be required to establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system, and monitor compliance with the mitigation measures put into place and the effectiveness of the same.
c. **Persons who make available for use, or manage the operation of, a high-impact system**: Persons making available for use, or managing the operation of, a high-impact system will need to publish on a publicly available website a plain language description of the system that will include explanations of how the system is intended to be used, the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make and the measures established to mitigate the risks of harm or biased output that could result from the use of the high-impact system.

D. What are the potential offences and penalties under AIDA? How is AIDA enforced?

If passed, AIDA will introduce new private-sector regulatory requirements with the aim of preventing harm resulting from AI systems. Once enacted, this means that businesses may face monetary penalties or criminal sanctions if they contravene AIDA, as further detailed herein.

General offences

Every person who contravenes any of the requirements noted above in Section 2(C) (*What is being regulated under AIDA?*) is guilty of an offence. Conviction in the most serious of cases could mean a fine of not more than the greater of CA$10 million and 3% of the person's gross global revenues in its immediately preceding financial year (for non-individuals, e.g., corporations) and a fine in the discretion of the court in the case of individuals.

Serious offences

AIDA puts a focus on severe ramifications where a person, without lawful excuse and knowing that (or being reckless as to whether) the use of an AI system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, makes the AI system available for use anyway, and such harm or damage occurs. In addition, a person who, with intent to defraud the public and cause substantial economic loss to an individual, makes an AI system available for use (and loss ensues) will be subject to serious consequences.

As currently drafted, a conviction following the commission of one or more of the above noted offences in the most serious of circumstances could mean a fine of not more than the greater of CA$25 million and 5% of the person's gross global revenues in its immediately preceding financial year (for non-individuals, e.g., corporations) and a fine in the discretion of the court in the case of individuals. A term of imprisonment is also a possibility for convicted individuals in certain circumstances.

Administrative monetary penalties

A person who is found under the regulations (which, as noted, have yet to be released) to have committed a violation is liable for an administrative monetary penalty to be established in the regulations. The purpose of these penalties is to promote and encourage compliance and not to punish. An act or omission may be proceeded with as a violation or as an offence, but proceeding with one precludes recourse to the other.

---

3 Canada, *Directive on Automated Decision-Making,* (Ottawa: President of the Treasury Board, 2021). <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592> accessed 7 July, 2022.

Potential costs to Canadian businesses

Businesses in Canada can expect increased costs associated with developing and deploying AI technologies, given that AIDA will mandate that private-sector businesses:

a. Adhere to data anonymization and management regulations;
b. Assess AI technologies to determine if they are high-impact as defined in AIDA;
c. Reduce and mitigate risk for high-impact AI systems;
d. Report actual or potential harm resulting from AI systems;
e. Cooperate with and pay for ministerial-ordered audits;
f. Comply with ministerial directives to implement safety measures, cease the use of a product, and publish information (excepting confidential business knowledge); and
g. Keep records related to these mandates.[4]

It is possible to forecast AIDA's potential impact on Canadian businesses, from a cost perspective, based on analyses of similar legislation in other jurisdictions. For example, in April 2021, the European Commission submitted its proposal for a European Union-based approach to AI that centers on excellence and trust and aims to boost research and industrial capacity while ensuring fundamental human rights. This proposal included communication on fostering a European approach to AI, a coordinated plan with European Union Member States, and the proposed *Artificial Intelligence Act* (the AIA), which is discussed in further detail below. Like AIDA, the AIA focuses on the specific utilization of AI systems and associated risks.

The AIA provides that businesses or public authorities that develop or use AI systems that constitute a high-risk to safety or to fundamental human rights (i.e., those that have a significant harmful impact on the health, safety and fundamental rights of persons in the European Union) are required to comply with mandatory requirements for trustworthy AI and to follow conformity assessment procedures before the AI systems can be placed on the European Union market.[5] These mandatory requirements will concern, among other things, traceability (i.e., the maintenance of a complete and detailed account of the development and functioning of an AI system), transparency (i.e., the provision of explanations of algorithmic models and decisions that are comprehensible for the user of the AI system), human oversight (i.e., the capability to oversee the overall activity of the AI system and the ability to decide when and how to use the AI system), and robustness (i.e., the ability of the AI system to withstand or overcome adverse conditions, including digital security risks). Obligations will also be placed on providers and users of AI systems to ensure safety and the respect of existing legislation protecting fundamental rights.[6] Compliance with these requirements and obligations will result in costs for businesses that develop or use AI.

Furthermore, under the AIA, providers of non-high-risk AI systems are encouraged to voluntarily apply the mandatory requirements for high-risk AI systems and to create and implement codes of conduct that may include voluntary commitments related to, among other things, environmental sustainability and accessibility for persons with disability. Any business-related changes required to meet these types of commitments would likely increase costs for a business.

In April 2021, the European Union published a legislative impact assessment that concluded that complying with the AIA's regulations would cause an additional 17% of overhead on all AI spending for businesses[7]. In July 2021, the Centre for Data Innovation (a non-profit think tank with staff in the U.S. and Belgium) noted that "the AIA will cost the European economy €31 billion over the next five years and reduce AI investments by almost 20%. A European SME [small to medium sized enterprise] that deploys a high-risk AI system will incur compliance costs of up to €400,000 which would cause profits to decline by 40%."[8] It also provided that the AIA will cause a 17% increase in overhead and out -of-pocket expenses on all AI spending in order to comply with the AIA. For example, a business with a €10 million turnover would see its profits fall by 40%. The Centre for Data Innovation also indicated that the macroeconomic costs of the AIA could be higher than projected, as its analysis did not consider unquantifiable costs resulting from AI regulation, e.g., deterring investment in AI, slowing economic digitization, deterring talent from working in a regulated environment, and placing national businesses at a competitive disadvantage compared to businesses operating in less restrictive jurisdictions such as China.

The International Data Corporation (a global information technology market research and analysis provider) conducted a study on Canadian AI software and platforms market revenue and concluded in 2020 that "[s]trong growth of approximately 16% per year is forecast for the Canadian AI software market over the 2020–2024 period."[9] As a result of AIDA, businesses may see this growth slow to some degree.

---

4 AIDA at s. 10.

5 "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (2021) at s. 1.1 and s. 3.3, online (pdf): The AI Act < https://artificialintelligenceact.eu/the-act/> [AIA].

6 *Ibid* at s. 1.1.

7 European Commission Directorate-General for Communications Networks, Content and Technology, "Study To Support An Impact Assessment Of Regulatory Requirements For Artificial Intelligence In Europe", (21 April 2021) at pg. 134, online: <http://dx.doi.org/10.2759/523404>.

8 Benjamin Mueller, "How Much Will the Artificial Intelligence Act Cost Europe?", Information Technology and Innovation Foundation (26 July 2021) at pg. 3, online: <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/>.

9 Warren Shiau, "Canadian Artificial Intelligence Software and Platforms Forecast, 2020–2024", International Data Corporation (December 2020), online: <https://www.idc.com/getdoc.jsp?containerId=CA45063020#:~:text=%22Strong%20growth%20of%20approximately%2016,and%20Analytics%20at%20IDC%20Canada>.

Comparison of AIDA to other global initiatives regarding AI

	AIDA[10]	Bill-64 (The Act to modernize legislative provisions respecting the protection of personal infromation)	National Institute of Standards and Technology's (NIST) AI Risk Management Framework[11]	European Commission's Ethics Guidelines for Trustworthy AI[12]	European Commission's White Paper on Artificial Intelligence[13]	*Artificial Intelligence Act*[14]
Purpose	To regulate international and interprovincial trade and commerce in AI systems and implement common requirements applicable across Canada for the design, development and use of AI systems. To prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests (Section 4). Notably: a. A person carrying out any regulated activity and who processes or makes available for use anonymized data in the course of those activities must establish measures with respect to the manner in which data is anonymized and the use or management of anonymized data (Section 6). b. A person who carries out any regulated activity must keep records describing in general terms, as the case may be, the measures established with respect to the anonymization of data and the use and management of the same, as well as risk assessment and mitigation measures taken with respect to high-impact systems. A record must also be kept of the reasons supporting an assessment of a system as being a high-impact system (Section 10). c. A person who is responsible for an AI system must assess whether it is a high-impact system (Section 7). d. A person who is responsible for a high-impact system must establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system, and must establish measures to monitor compliance with the mitigation measure established and the effectiveness of the same (Section 9). e. A person who is responsible for a high-impact system must notify the Minister if the use of the system results or is likely to result in material harm (Section 12).	To modernize the framework applicable to the protection of personal information (Explanatory notes to Bill 64).	To address AI risks, guide the development and use of trustworthy and responsible AI, and improve understanding of and help organizations manage both enterprise and societal risks related to the development, deployment, and use of AI systems (Section 1, page 1). Use is voluntary, and it is made for a broad scope of "individuals and organizations, regardless of sector, size, or level of familiarity with a specific type of technology" (Section 3).	To set out a framework for achieving trustworthy AI by offering guidance on fostering and securing ethical and robust AI (page 2). Notably, it creates a "Trustworthy AI Assessment List" aimed at operationalizing its key requirements (Chapter III, page 26).	To present policy options to enable a trustworthy and secure development of AI in Europe, respecting the values and rights of EU citizens, based on a policy framework to achieve an "ecosystem of excellence," and elements of a future regulatory framework for AI in Europe that will create a unique "ecosystem of trust" (page 3).	To lay out: a. Harmonized rules for the placing on the market, the putting into service and the use of AI systems in the EU; b. Prohibitions of certain artificial AI practices; c. Specific requirements for high-risk AI systems and obligations for operators of such systems; d. Harmonized transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorization systems, and AI systems used to generate or manipulate image, audio or video content; and e. Rules on market monitoring and surveillance (Article 1).

10 Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022) [*AIDA*].

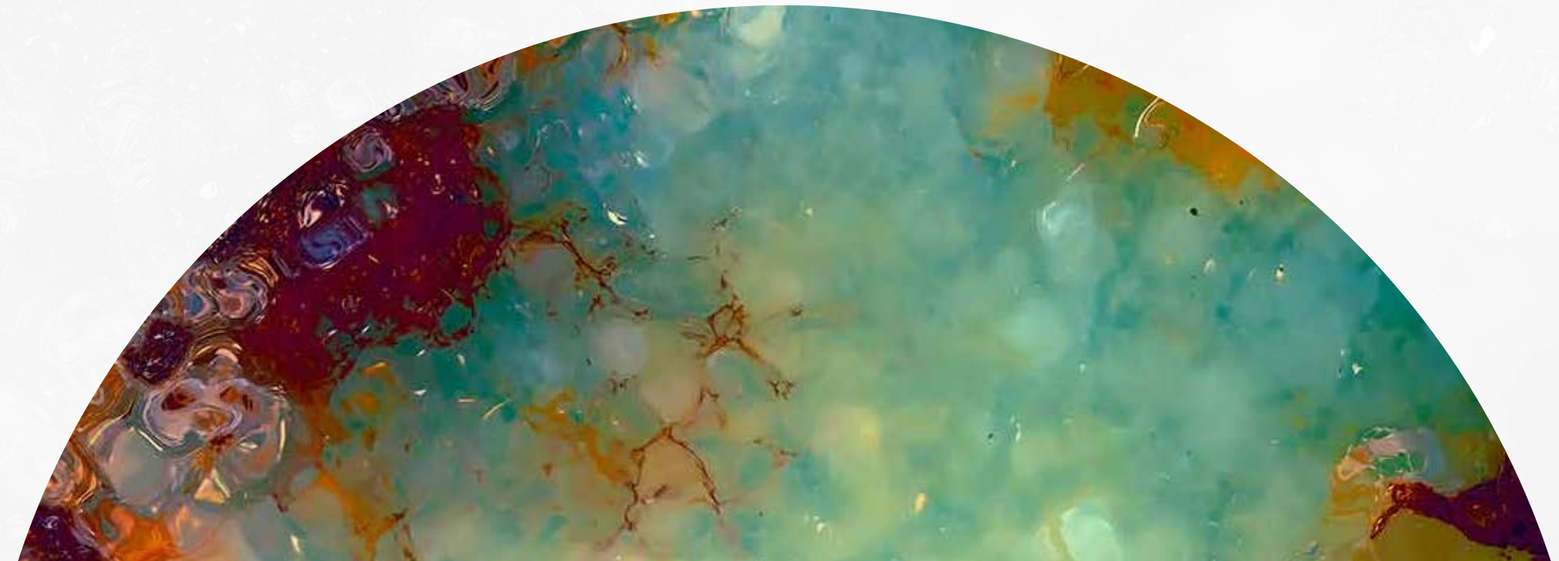
11 National Institute of Standards and Technology, "AI Risk Management Framework: Initial Draft" (2022), online (pdf): *NIST* < https://www.nist.gov/itl/ai-risk-management-framework> [AI RMF].

12 Independent High-Level Expert Group on Artificial Intelligence Set Up by the European Commission, "Ethics Guidelines for Trustworthy Artificial Intelligence (AI)" (2019), online (pdf): *European Commission* <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html> [EU Ethics Guidelines].

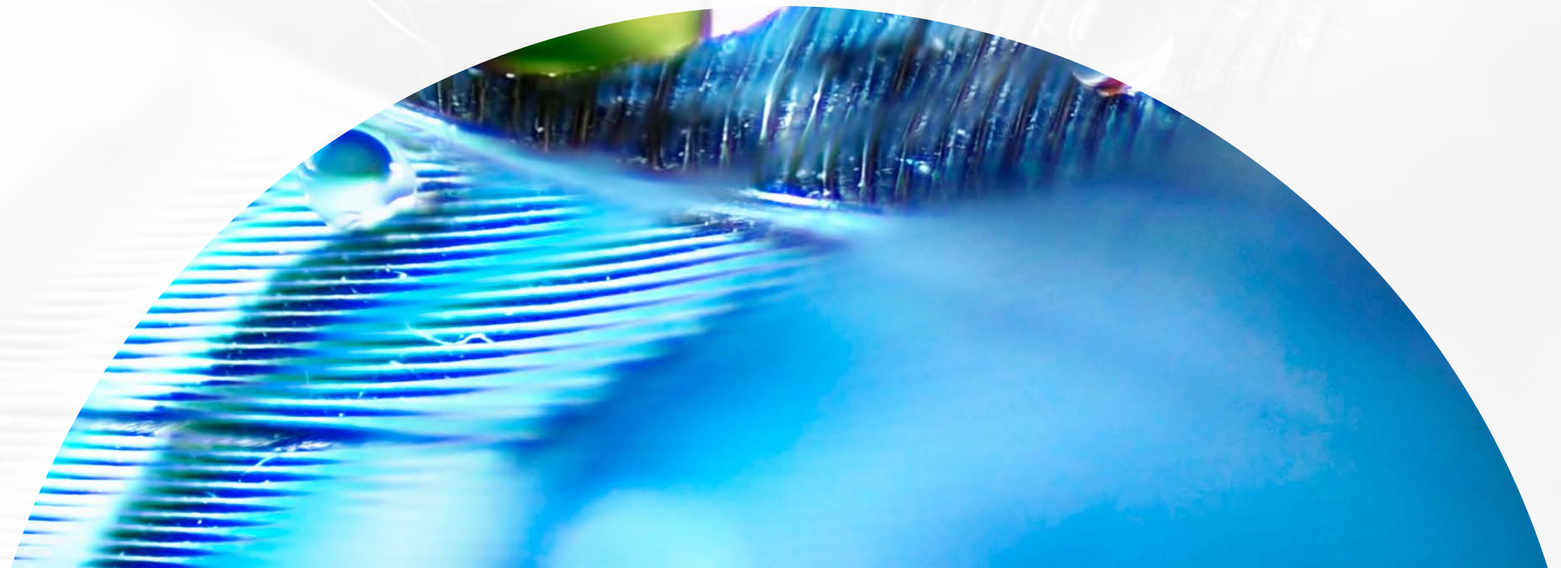
13 European Commission, "White Paper on Artificial Intelligence – A European Approach to excellence and Trust" (2020), online (pdf): *European Commission* < https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [White Paper].

14 European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (2021), online (pdf): *The AI Act* <https://artificialintelligenceact.eu/the-act/> [AIA].

Jurisdiction	Canada.	Québec, including all enterprises and their suppliers collecting, holding, using or communicating personal information of individuals in Québec.	United States.	Member States of the EU (with aspirations of applying outside the EU).	Member States of the EU.	Member States of the EU.
Definition of artificial intelligence OR Artificial intelligence system(s)	**"Artificial intelligence system"** means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions (Section 2).	The use of personal information to render a decision based exclusively on an automated processing of such information (Section 12.1).	**"Artificial intelligence"** means algorithmic processes that learn from data in an automated or semi-automated manner (Section 1, page 2).	**"Artificial intelligence systems"** means software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions (page 36).	**"Artificial intelligence"** means a collection of technologies that combine data, algorithms and computing power (page 2).	**"Artificial intelligence system"** means software developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate content, predictions, recommendations, or decisions influencing the environments they interact with (Article 3).
Scope of application	Any person, which includes a trust, a joint venture, a partnership, an unincorporated association and any other legal entity, engaging (in the course of international or interprovincial trade of commerce) in the: a. Processing or making available for use any data relating to human activities for the purpose of designing, developing or using an AI system; and/or b. Designing, developing or making available for use an AI system or managing its operations (Section 2; Section 5(2)). Notably, the range of persons to which AIDA applies is quite broad and will include designers, developers and providers of AI systems; however, a "person" is unlikely to include the AI system itself as AI does not currently have legal personality.	Natural persons and enterprises, enterprises meaning "the carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or altering property, or providing a service" (Section 1525 of the *Québec Civil Code*).	Individuals and organizations of all sectors, sizes, or familiarities with a specific type of technology who are developing and using AI (Section 2, page 2). Four stakeholder groups are listed as intended audiences: AI system stakeholders, operators and evaluators, external stakeholders, and the general public (Section 3, page 4).	All AI stakeholders designing, developing, deploying, implementing, using or being affected by AI, including but not limited to companies, organizations, researchers, public services, government agencies, institutions, civil society organizations, individuals, workers and consumers can opt to use these guidelines (Section A, page 5).	The working assumption is that the regulatory framework would apply to developers and deployers of products and services relying on AI (page 10, page 16).	Providers in the EU (regardless of whether they are established in the EU), users of AI systems located within the EU, and "providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union" – an extraterritorial application (Article 2(1)).



Assessment and risk mitigation measures	A person who is responsible for an AI system must, in accordance with the regulations, assess whether it is a high-impact system (Section 7). A person who is responsible for high-impact systems must establish measures to identify, assess, and mitigate the risks of harm or biased output that could result from the use of the system (Section 8).	Privacy impact assessments (Section 3.3), the duty to inform individuals (Section 8.1) and the duty to provide: a. A description of personal information used; b. Reasons and principal factors and parameters for the decision; c. Right of access to that personal information; and d. The opportunity for the individual to present observations to a person who is in a position to review the decision (Section 12.1).	Does not prescribe risk thresholds or values; instead, lets organizations specifically define their risk thresholds and manage those risks within their tolerances (Section 4.2.2, page 6). Characteristics of risk management approaches can be classified according to the following: a. Technical characteristics: accuracy, reliability, robustness, resilience or security; b. Socio technical characteristics: explainability, interpretability, privacy, safety, and managing bias; and c. Guiding principles: fairness, accountability, transparency (Section 5, Figure 3, page 8).	Acknowledges that, while bringing substantial benefits to individuals and society, AI systems also pose certain risks and may have a negative impact, including impacts which may be difficult to anticipate, identify or measure (page 14). Organizations should adopt adequate measures to mitigate these risks when appropriate, and proportionately to the magnitude of the risk (page 14). Provides a non-exhaustive assessment list to guide AI practitioners to achieve trustworthy AI (page 25): a. Human agency and oversight; b. Technical robustness and safety; c. Privacy and data governance; d. Transparency; e. Diversity, non-discrimination and fairness; f. Societal and environmental well-being; and g. Accountability (pages 26-31).	Current product safety legislation could include provisions explicitly covering new risks presented by the emerging digital technologies, to provide more legal certainty about risks arising from products (page 15). In addition to possible adjustments to existing legislation, new legislation specifically regarding AI may be needed in order to make the EU legal framework fit for the current and anticipated technological and commercial developments (page 16). A risk-based approach is necessary to ensure regulatory intervention is appropriate. The risk determination should be clear and easily understandable and applicable for all parties concerned. High-risk applications should be considered in light of what is at stake, considering both the risks associated with the intended sector and use—particularly regarding the safety, consumer rights and fundamental rights. (page 17) Provides two suggested criteria for high-risk AI application: a. Use is in a sector where significant risk is expected (e.g., healthcare; transport; energy and parts of the public sector); and b. Use is in a manner where significant risk is likely to arise e.g., impact on affected parties—legal risks or safety risks (e.g., risk of physical injury) (page 17). All reasonable measures should be taken to minimize the risk of harm being caused, which could include: a. Mitigating measures in case of attempts to manipulate AI systems; b. Human oversight; and c. Specific requirements for remote biometric identification (page 21).	Differentiates between uses that create (i) an unacceptable risk, which is prohibited (ii) a high-risk, which is permitted subject to the below requirements and (iii) low or minimal risk, which is permitted with no restrictions (Article 4, Article 9). High-risk AI systems that pose significant risks to the health and safety or fundamental rights of persons will have to comply with a set of mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the EU market (Part 1.1, page 3). A risk management system in relation to high-risk AI systems is required (Article 9(1)). High-risk AI systems shall be tested to identify the most appropriate risk management measures (Article 9(5)).



Monitoring requirements	A person responsible for a high-impact system must, in accordance with the regulations, establish measures to monitor compliance with the mitigation measures and the effectiveness of those mitigation measures (Sections 8 and 9).	Not generally applicable, although the right of individuals to access the personal information used and to make representations to a person in a position to review the decision may provide a form of monitoring (Section 12.1).	Operators and evaluators will provide monitoring and formal/informal test, evaluation, validation, and verification (TEVV) of system performance, relative to both technical and socio-technical requirements (Section 3, page 4). The appropriateness of metrics and effectiveness of existing controls should be regularly assessed and updated (Section 6.2, page 17). Responses to risks should be documented and monitored. Post deployment monitoring of systems may need to be implemented, including mechanisms for user feedback, appeal and override, decommissioning, incident response, and change management (Section 6.3, page 17). Governance processes on potential impacts of AI technologies should focus on both the technical side of AI systems, and the organizational practices impacting individuals who monitor the systems (Section 6.4, page 18). Policies and procedures to address AI risks arising from supply chain issues, including third-party software and data may need to be in place (Section 6.4, page 19).	There may be a separate process implemented to monitor the AI system's compliance with "white list" rules (behaviours or states) that the system should always follow, "black list" restrictions on behaviours or states that the system should never transgress, and mixtures of those or more complex provable guarantees regarding the system's behaviour (Section 2.1).	The data that AI systems are trained on should be monitored to ensure that they are sufficiently broad and cover all relevant scenarios needed to avoid dangerous situations (page 19). Legal requirements to impose may require human oversight, which includes monitoring of the AI system while in operation and the ability to intervene in real time and deactivate (e.g., a stop button or procedure is available in a driverless car when a human determines that car operation is not safe) (page 21).	Providers of AI systems shall establish and document a post-market monitoring system in a manner proportionate to the nature of the AI technologies and the risks of the high-risk AI system (Article 61).

Transparency requirements	The person who makes a high-impact AI system available for use must make a plain-language description of the system that includes an explanation of the following information publicly available: a. How the system is intended to be used; b. The types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make; c. The mitigation measures established in respect of it; and d. Any other information that may be prescribed by regulation (Section 11). The person who manages a high-impact AI system must make a plain-language description of the system that includes an explanation of the following information publicly available: a. How the system is used; b. The types of content that it generates and the decisions, recommendations or predictions that it makes; c. The mitigation measures established in respect of it; and d. Any other information that may be prescribed by regulation (Section 12).	Use of the technology and personal information used, reasons, principal factors and parameters that led to the decision and right to access the personal information used (Sections 8.1 and 12.1).	Transparency is a guiding principle relevant to AI risk, necessary for actionable redress related to incorrect and adverse AI system outputs (Section 5.3, page 13). Transparency reflects the extent to which information is available to a user when interacting with an AI system and prevents users from being left to make guesses and assumptions about aspects of an AI system's design and deployment (Section 5.3.3, page 13). Policies, processes, procedures and practices across the organization related to the development, testing, deployment, use and auditing of AI systems should be transparent. Risk management processes and outcomes should be documented and traceable through transparent mechanisms, as appropriate and to the extent practicable (Section 6.4, page 19).	Transparency requirements are linked to the principle of explicability and includes traceability, explainability, and communication (Section 1.4). Traceability requires documenting the data sets and processes that yield the AI system's decision, including those of data gathering and data labelling as well as the algorithms used (page 18). Explainability concerns the ability to explain both the technical processes of an AI system and the related human decisions (e.g., application areas of a system) (page 18). The decisions of an AI system should be understandable and traceable by human beings. Whenever an AI system has a significant impact on people's lives, it should be possible to demand a suitable explanation of the AI system's decision-making process that is timely and adapted to the expertise of the stakeholder concerned. Explanations of the degree to which an AI system influences and shapes the organisational decision-making process, design choices of the system, and the rationale for deploying it, should be available (hence ensuring business model transparency) (page 18). Communication means AI systems should be identifiable, and humans should be informed that they are interacting with an AI system. The option to decide against this interaction in favour of human interaction should be provided where needed to ensure compliance with fundamental rights. An AI system's capabilities and limitations should be communicated to AI practitioners or end-users (page 18).	Clear information on the AI system's capabilities and limitations, in particular the purpose for which the systems are intended, the conditions under which they can be expected to function as intended, and the expected level of accuracy in achieving the specified purpose should be provided to deployers of the systems, and possibly competent authorities and affected parties. Additions to existing data protection rules may be required to ensure citizens are informed when they are interacting with an AI system and not a human being (page 20).	For high-risk AI systems, high-quality data, documentation and traceability, transparency, human oversight, accuracy and robustness are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI and that are not covered by other existing legal frameworks (Part 2.3). Importers of high-risk AI systems should ensure that the system bears the required conformity marking and is accompanied by the required documentation and instructions of use (Article 26). Before placing on the market or putting into service a high-risk AI system, the provider or authorized representative shall register that system in the EU database (Articles 51 and 60). High-risk AI systems shall be designed and developed to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately (Article 13). Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence (Article 52).

Record keeping requirements	A person who carries out any regulated activity must, in accordance with the regulations, keep records generally describing the measures they establish and the reasons supporting their assessment (Section 10(1)). The person must, in accordance with the regulations, keep any other records about requirements that apply to them regarding anonymized data, risk assessment, monitoring of mitigation measures, and the reasons supporting their assessment as to whether an AI system is a high-impact system (Section 10(2)).	Not applicable.	Impacts of AI system use and responses to measured risks may need to be documented over time (Section 6.1, page 15; Section 6.3, page 18). Risk management processes and their outcomes may be documented to the extent practicable, and teams are encouraged to document the impacts of the technology they desig, and to communicate these impacts (Section 6.4, page 19).	On the Trustworthy AI Assessment list, items that should be recorded include documentation of processes for testing and verification of the reliability of AI systems, methods used to design and develop algorithmic systems, and trade-offs between relevant interests and values implicated by the AI system (page 28, 31).	The regulatory framework should require record-keeping of the following: a. The data set used to train and test the AI systems, including a description of the main characteristics and how the data set was selected; in certain justified cases, the data sets themselves; and b. Documentation on the programming and training methodologies, and processes and techniques used to build, test and validate the AI systems, including where relevant in respect of safety and avoiding bias that could lead to prohibited discrimination (page 19). Records and data sets should be retained for a limited, reasonable time (page 19).	Records and technical documentation with information necessary to assess compliance of the AI system with the relevant requirement should be kept up to date. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used and documentation on the relevant risk management system. (Clause 46, page 30). Technical documentation of a high-risk AI system shall be drawn up before being placed on the market or put into service and shall be kept up-to-date (Article 11). High-risk AI systems should be accompanied by relevant documentation and instructions of use and shall include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate (Clause 47, page 30). Logging capabilities shall provide, at a minimum: recording of the period of each use of the system (start date and time and end date and time of each use); the reference database against which input data has been checked by the system; the input data for which the search has led to a match; and the identification of the natural persons involved in the verification of the results (Article 12).
Notification requirements	Persons who are responsible for high-impact AI systems must notify the Minister if use of the system results or is likely to result in material harm (meaning physical or psychological harm to an individual, damage to an individual's property or economic loss to an individual) (Section 12). If it is in the public interest, the Minister may publish non-confidential information about any contravention of AIDA on a publicly available website (Section 27(1)). Without the consent of the person to whom the information relates and without notifying that person, the Minister may publish, on a publicly available website, non-confidential information that relates to an AI system if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm; and the publication of the information is essential to prevent the harm (Section 28(1)).	Individuals must be informed of the use of technology that includes functions allowing the identification, location and profiling of individuals and of the means available to activate these functions (Section 8.1).	Not applicable.	The "Privacy and data governance" section of the Trustworthy AI Assessment List concerns building in mechanisms for notice and control over personal data, depending on the use case (such as valid consent and possibility to revoke, when applicable) (page 28).	Adequate information about the use of high-risk AI systems should be provided in a proactive manner (page 20). Citizens should be clearly informed when they are interacting with an AI system and not a human being. The information should be objective, concise and easily understandable, and the information provided should be tailored to the context (page 20).	Each member state shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. Conformity assessment bodies shall apply for notification to the notifying authority of the member state in which they are established (Articles 30-39).

Use of anonymized data	A person who carries out any regulated activity and who processes or makes available for use anonymized data in the course of that activity must, in accordance with the regulations, establish measures with respect to the manner in which data is anonymized, and the use or management of anonymized data (Section 6).	Limited to "serious and legitimate purposes" (Section 23).	Not applicable.	The "privacy and data governance" section of the Trustworthy AI Assessment List contains the question, "Did you take measures to enhance privacy, such as via encryption, anonymisation and aggregation?" (page 28). The use of "anonymous" personal data that can be re-personalized raises the concern of developing ways to allow meaningful and verified consent to be given to AI technologies, and automatically identified by AI or equivalent technologies (page 34).	AI poses risks for fundamental rights, as it may be used to retrace and de-anonymise personal data, affecting rights to free expression, personal data protection, privacy, and political freedoms (page 11).	Where strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in the regulations, subject to appropriate safeguards, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymization, or encryption where anonymisation may significantly affect the purpose pursued (Article 10(5)).
Enforcement	Administrative monetary penalties: A person who is found under the regulations to have committed a violation is liable to the administrative monetary penalty established by the regulations (Section 29). Criminal offences: Contravention of requirements: A person who contravenes any of the above requirements is liable to a maximum fine of the greater of CA$10 million and 3% of the person's gross global revenues in the preceding year or, in the case of an individual, a fine in the discretion of the court (Section 30). Criminal offences: Related to AI systems: The following prohibited activities are criminal offences: a. Unlawful use of personal information in AI systems; and b. AI systems which cause harm or economic loss (Section 38). A person who commits either of the above offences is liable to a maximum fine of the greater of CA$25 million and 5% of the person's gross global revenues in the preceding year or, in the case of an individual, a fine at the discretion of the court and/or a term of imprisonment of up to five years less a day (Section 40).	A monetary administrative penalty may be imposed by the Commission d'accès à l'information (CAI) for violation of the provisions of CA$50,000 in the case of a natural person, and CA$10 million or, if greater, 2% of worldwide turn over of the preceding year, in all other cases (Sections 90.1 and 90.12). A criminal offence is punishable by a fine of CA$5,000 to CA$100,000 for a natural person, and CA$15,000 to CA$25 million or, if greater, 4% of worldwide turn over of the preceding year (Section 91).	Accountability structures may need to be in place to ensure that the appropriate teams and individuals are empowered, responsible, and trained for managing the risks of AI systems (Section 6.4, page 19).	It must be ensured that public enforcers have the ability to exercise oversight in line with their mandate. Required oversight mechanisms may vary depending on the AI system's application area and potential risk. The less oversight a human can exercise over an AI system, the more extensive testing and stricter governance is required (Section 1.1, page 16).	The opacity of AI makes enforcement more difficult. Legislation should be examined as to whether it can address the risks of AI and be effectively enforced, whether adaptations of the legislation are needed, or new legislation is needed (page 10). Record-keeping requirements should facilitate enforcement (page 18).	An individual may be fined up to €30 million and a company may be fined up to 6"% of its total worldwide annual turnover for the preceding financial year, whichever is higher (Article 71).

Authored by Tom Sides, John Lemieux, Jaclin Cassios and Rachel Macklin. The authors would also like to thank the following summer students for all their hard work in preparing this insight: Thomas Banks, Anu Chadha, Tamya Chowdhury and Sarah Fong.

CSBrand-94614-Part three of Canada's new federal privacy Bill C-27-Artificial Intelligence and Data Act-09 — 26/07/2022