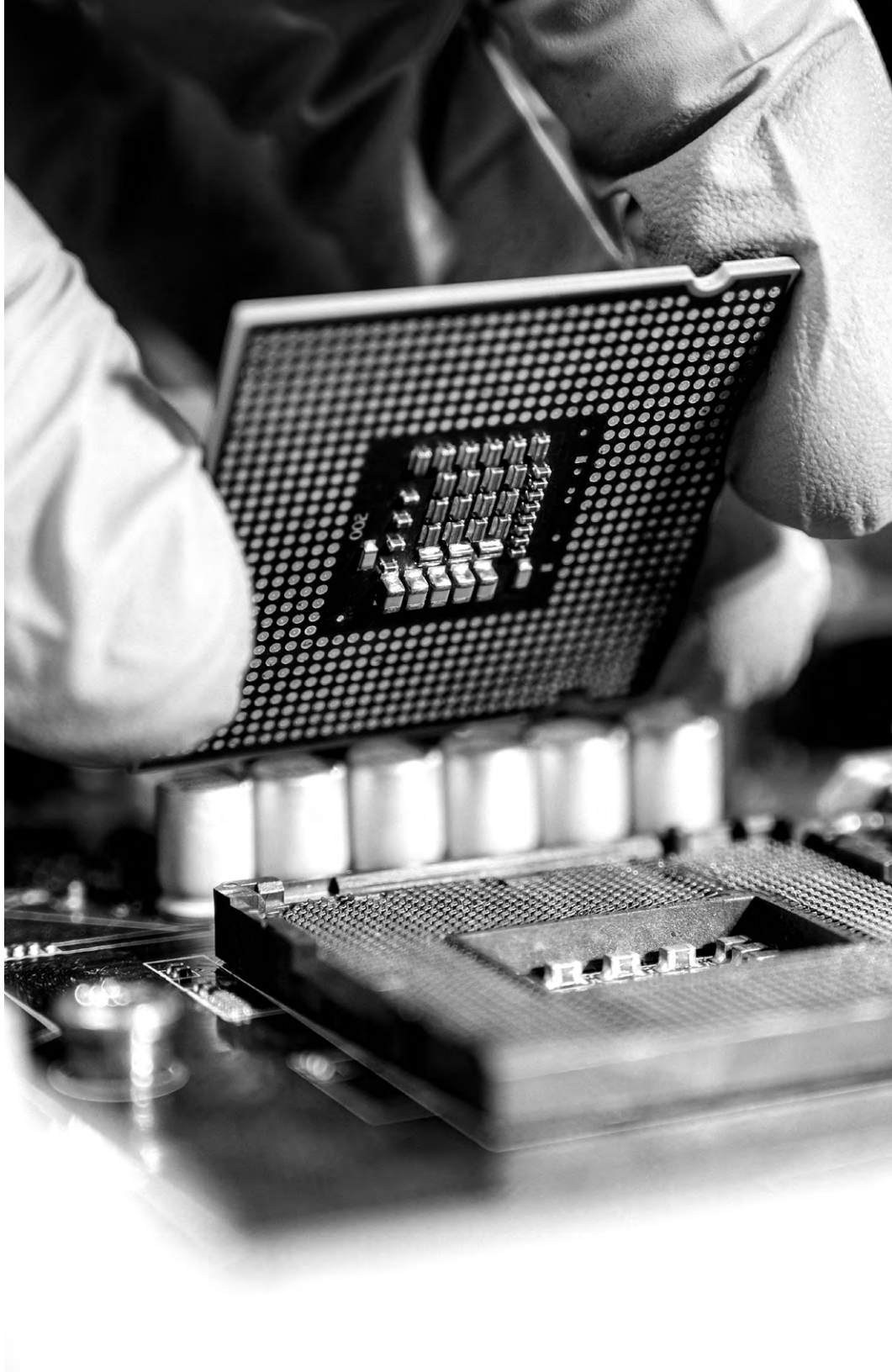
Navigating 2026: Key trends shaping the Technology Sector



FASKEN

Own tomorrow

Contents

Trend #1: Agentic AI Will Continue to Expand the Frontier of Automation, Prompting Organizations to Balance Innovation with Rigorous Legal, Governance, and Operational Controls

The key factor that distinguishes agentic AI from other iterations of artificial intelligence is that it is a system that can accomplish a specific goal autonomously – i.e., understanding, planning, and executing tasks all without human intervention. By way of comparison, generative AI (one of the trending forms of AI in the past few years) focuses on *creating content* based on learned patterns and agentic AI goes a step further by taking this content and *completing an action*.[1] For example, agentic AI can tell you the best time to fly for your trip and help you build an itinerary, but also book your flight and accommodations on your behalf.

EMERGING ADOPTION

The Agentic Enterprise Salesforce Index[2], which surveyed AI usage from a cohort of businesses using Salesforce's platform data found that the top three most popular use cases for AI agents are customer service, internal business automation, and sales. In sales, drafting and sending emails are the top agent actions, followed by developing to-dos and scheduling meetings. Another report from November 2025 by McKinsey[3] on the state of AI found that 23% of respondents are scaling an agentic AI system somewhere in their enterprises (that is, expanding the deployment and adoption of the technology within at least one business function), and an additional 39% say they have begun experimenting with AI agents. Use of AI agents is most commonly reported in IT and knowledge management (e.g., service-desk management in IT and deep research in knowledge management).

The key takeaway is that use of AI agents is not widespread *yet*. Agents are being used for specific functions and tasks, and in any given business function, no more than 10% of respondents say their organizations are scaling AI agents. The findings suggest that organizations are largely curious about agentic AI and are still experimenting with it (approximately 62% of respondents).[4]

Gartner predicts that organizations are in a crucial three- to six-month window to define agentic AI product strategies. The AI industry has reached an adoption inflection point, with Gartner projecting that 40% of enterprise applications will include integrated task-specific agents by 2026 (up from 5% in August 2025).[5]

1. See more information regarding the capabilities of agentic AI and the differences between agentic AI and generative AI here: IBM - What is agentic AI? and IBM - AI agents in 2025: Expectations vs. reality.
2. Full index: Salesforce - The Agentic Enterprise Index.
3. Full report: McKinsey - The state of AI in 2025: Agents, innovation, and transformation.
4. Ibid.
5. Full press release: Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025.

SETTING CLEAR BOUNDARIES AROUND HOW AND WHERE TO DEPLOY AGENTIC AI

Organizations should have a clear understanding of the capabilities of the agentic AI systems they engage with and clearly define boundaries for what they will allow agentic AI to do autonomously and which other tasks still require human involvement and real-time oversight. Low-risk, repetitive, and easily automated tasks are appropriate for agentic AI,[6] whereas sensitive, complicated or high-risk applications warrant greater caution.

A Note on Marketing Liability

A related challenge arises when organizations, or the vendors they rely on, overstate the true level of autonomy that their AI systems can provide. Whether developing AI products marketed as "agentic" or procuring tools that claim to be agentic, organizations must assess how autonomous the product truly is before launching or purchasing it.

While the Federal Trade Commission (FTC) in the US has been cracking down on deceptive AI claims generally, recent FTC activities reveal that "AI washing" is trending upward. In August 2025, the FTC sued Air AI (a company selling business coaching and support services) for making a number of misleading claims about its AI product, including that it can operate autonomously and "replace human customer service representatives and, in combination with other services, make business owners significant sums of money".[7] In reality, the FTC alleged that the AI technology frequently failed to perform basic functions like placing outbound calls, scheduling appointments, recording email addresses, or responding accurately to questions.[8]

6. IBM - AI agents in 2025: Expectations vs. reality.
7. Full press release: FTC Sues to Stop Air AI from Using Deceptive Claims about Business Growth, Earnings Potential, and Refund Guarantees to Bilk Millions from Small Businesses.
8. Full FTC claim: Federal Trade Commission v. Air Ai Technologies Incorporated (2:25-cv-03068) at para 51.

UNIQUE AI GOVERNANCE CHALLENGES

Beyond the typical governance issues that apply to AI adoption generally, agentic AI raises some unique concerns that organizations should be aware of.

1. Managing Liability

Organizations will need to shift their focus from erroneous *content* to improper *actions*. Traditional law of agency – where another human or corporation acts as an agent on behalf of an organization – generally requires that the principal is responsible for the actions of its agents. In the case of agentic AI, organizations should assume that similar liability applies by default. However, when contracting with vendors, organizations should consider how this liability can be shared with the developers and/or distributors of agentic AI to reduce liability. For example, organizations may push back on warranties that the agent is made available on an "as is" basis and may require certain warranties or service levels covering accuracy, training and availability. That said, at this stage, there is a general hesitancy in the market for vendors to make such commitments, and this may be difficult to negotiate where the vendor has greater bargaining power. Additionally, a customer should consider requiring vendors to provide an indemnity that covers any liability that may arise from improper actions taken by the agentic AI system.

2. Explainability

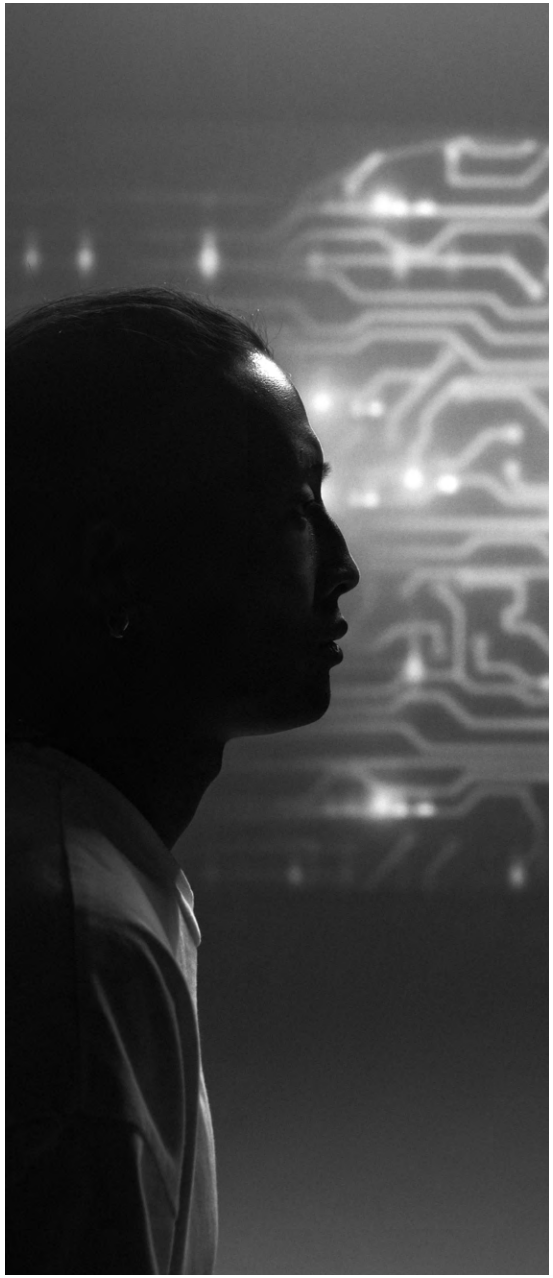
AI regulations throughout the world, both in force and proposed (including Canada's now-defunct *Artificial Intelligence and Data Act*) have consistently sought to address the ethical principles of explainability and transparency. Despite the absence of a comprehensive AI regulation in Canada to date, organizations should expect that some level of explainability will be required, especially where AI agents are used in consumer-facing applications or to make decisions about individuals.

It will be prudent to establish robust audit trails and activity logging for every decision made and action taken. Organizations will also need to demonstrate their ability to evaluate and verify each step of the workflow and ensure that monitoring and evaluation capabilities are built-in to detect errors, improve performance, and provide visibility into how the system operates.

3. Human Oversight

As agentic AI may rely on generative AI models, it is likely to be susceptible to the same types of hallucinations and other issues encountered when using generative AI in non-agentic applications. While agentic AI is by design intended to be autonomous, organizations should still consider implementing some degree of direct human oversight to minimize the impact of errors that may arise. This will especially be the case as organizations explore more complex use cases for agentic AI.

One question organizations should ask agentic AI vendors is whether they provide a managed service to address the need for human oversight. The vendor might be better equipped to readily understand certain logged data and act more efficiently in troubleshooting.



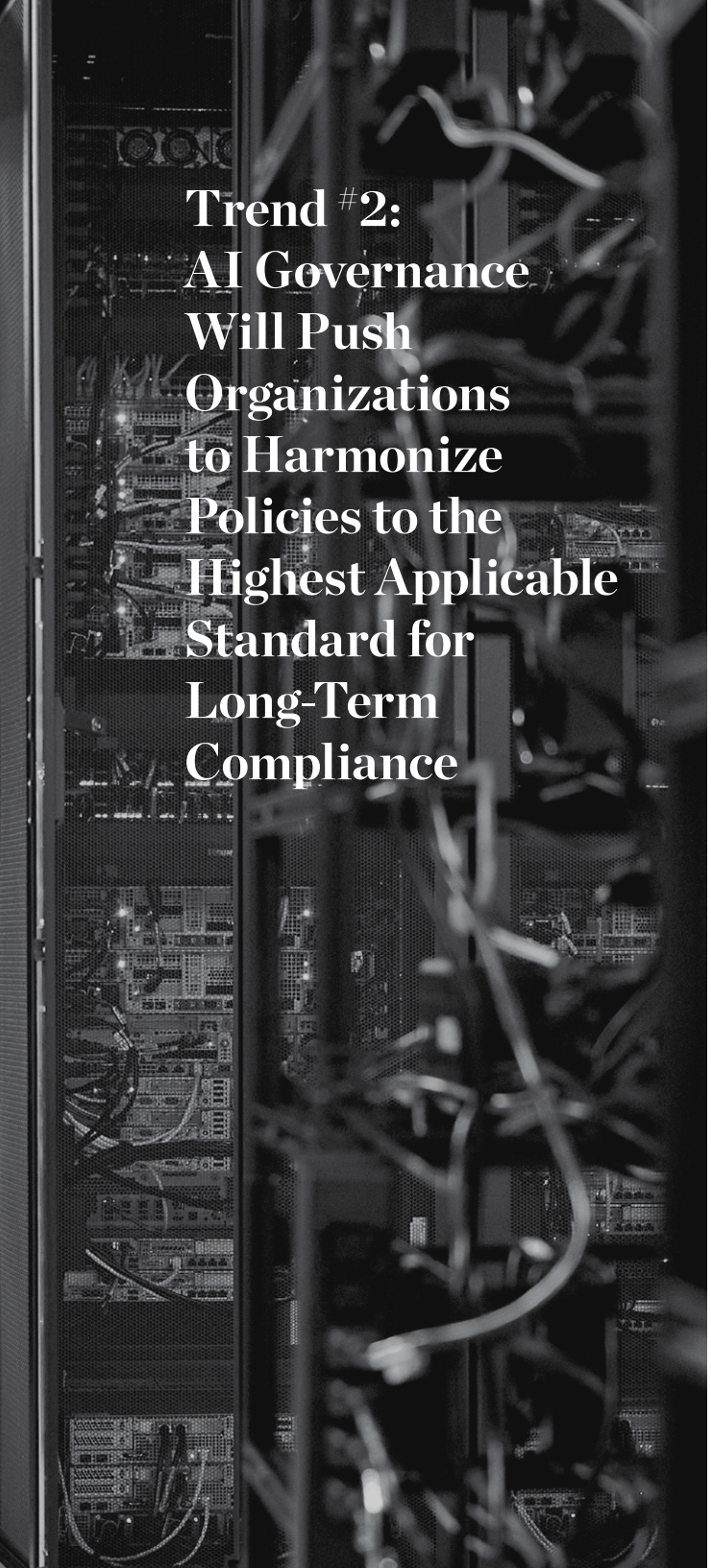
4. Testing

Given the ability of agentic AI to act autonomously, organizations should carefully consider testing standards and ensuring that AI agents are rigorously stress-tested in sandbox environments,[9] with sufficiently large sample sizes. This testing process, especially continuous testing during operation, is one way to maintain human oversight.

In addition to the obligations around accuracy discussed above, organizations should require an ongoing representation and warranty that the agent will continue to be accurate and perform in accordance with the agreement (including the technical specifications and the user documentation), even after updates are made, use cases change, or datasets are updated. Ongoing testing will be a key evaluation tool to ensure continuous accuracy.

Agentic AI represents the next major evolution in enterprise automation, one that shifts organizations from passively generating information to actively executing tasks with minimal human involvement. As organizations explore these opportunities, they must balance innovation with careful governance. Clear capability boundaries, responsible marketing practices and robust oversight frameworks will be critical to managing the heightened legal, operational, and ethical risks introduced by autonomous action. Ultimately, organizations that invest early in thoughtful testing, explainability measures, and shared liability models will be best positioned to leverage agentic AI safely and strategically.

9. IBM - AI agents in 2025: Expectations vs. reality.



Trend #2: AI Governance Will Push Organizations to Harmonize Policies to the Highest Applicable Standard for Long-Term Compliance

In 2026, we are well beyond the initial hype surrounding AI (particularly generative AI) and past the early uncertainty about whether preliminary use cases would mature into practical solutions. While Canada finds itself in a regulatory gap following the failure of Parliament to pass the *Artificial Intelligence and Data Act* (AIDA), the EU AI Act will be largely in force by August 2026, and the current US administration has introduced a "minimally burdensome" national framework that supersedes stricter state-level rules. We can also expect to see at least initial judgments in key AI lawsuits. As a result, 2026 may well be a year in which the focus turns to AI governance and compliance.

Canada's approach to the governance of AI development in 2026 follows a year in which the focus shifted away from a previous model of centralized federal oversight toward a multi-jurisdictional model characterized by provincial legislation, sectoral guidance, and voluntary industry codes. This shift was triggered by the prorogation of Parliament on January 6, 2025 which resulted in the end of Bill C-27 and AIDA. In the months that followed, the federal government adopted an approach to AI governance that places less emphasis on comprehensive national regulation, while some provinces such as Ontario and Québec have promoted their provincial AI governance frameworks, both within the public sector alone (see Ontario) and in the public sector and more broadly (see Québec). In all provinces (other than Ontario and Québec), as well as federally, AI is currently governed through privacy, human rights and sector- specific laws.

The practical impact has been a shift from a common federal approach to one that demands greater reliance on individual entities' own policies, processes and controls to guide their development, deployment and monitoring of AI systems, as well as ensuring for themselves that such controls remain sufficient, lawful, ethical and aligned with organizational objectives. In 2026, organizations will continue to develop needed internal controls and, in doing so, will need to meet the highest provincial requirements across the jurisdictions in which they operate.

FEDERAL VOLUNTARY CODE

At the federal level, the primary AI governance mechanism will likely remain the *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems*, which was first published in September 2023 and expanded in 2025. The Voluntary Code sets out six principles – accountability, safety, fairness and equity, transparency, human oversight, and validity and robustness – that apply to both developers and deployers of advanced generative AI systems.

The Voluntary Code does not provide enforcement mechanisms, investigation powers, or penalties for non-compliance. Instead, many organizations have chosen to abide by the Voluntary Code under the expectation that clear, consistent, and enforceable obligations will come from provincial legislation.

PROVINCIAL COMPLIANCE

In 2026 companies will continue to develop and refine their organizational policies on AI governance, in many cases to align with the highest applicable provincial standards across their enterprise.

Regulation in Ontario and Québec[10] primarily expands on existing privacy and cybersecurity laws. For example, Ontario's *Strengthening Cyber Security and Building Trust in the Public Sector Act*[11] initiated important change in governance strategies in the public sector as covered entities had to (i) provide transparent information about their use of AI systems, (ii) implement prescribed risk-management procedures, and (iii) develop accountability frameworks governing AI deployment. Whereas 2025 was a year of implementation for much of the *public* sector as they adjusted to the new rules and guidelines, 2026 should see ripple effects through the *private* sector. The compliance requirement imposed by public sector entities on the private organizations that they deal with will shift the compliance standard for everyone. We will see increasingly similar standards of transparency, risk management, and accountability, which may prompt private sector organizations to align their practices with the evolving expectations of the public sectore.

Other provinces have also addressed AI and automated decision-making,[12]; however, Québec's Law 25 has presented Canada's most comprehensive provincial framework on AI governance.

In 2026, companies will continue to develop and refine their organizational policies on AI governance, and we expect that organizations will continue to align with Québec Law 25's broader protection of personal information requirements found in the Act respecting the protection of personal information in the private sector to: (i) disclose when personal information is processed through automated systems, (ii) explain decision factors and criteria, (iii) enable contestation of decisions, and (iv) provide mechanisms for correcting inaccurate data. Penalties for violations may reach $25 million or four percent of global revenue across their operations to streamline compliance and customer communications.

10. See, for example, the *Enhancing Digital Security and Trust Act*, 2024, . 2024, c. 24, Sched. 1 or the Implementation guide for managers of Artificial intelligence systems.
11. Entered into force on January 29, 2025.
12. Alberta has advanced its regulatory measures through Bills 33 and 34 (effective December 5, 2024). These Bills amended the province's Freedom of Information and Protection of Privacy Act to require public bodies using personal information in automated decision-making to ensure data accuracy and retain processing records for at least one year.

SECTORAL GOVERNANCE OVERSIGHT

Canada's sectoral regulators have likewise advanced AI-specific obligations within their respective oversight frameworks.

For example, in the health sector, Health Canada's pre-market guidance for machine-learning-enabled medical devices, finalized in February 2025, requires manufacturers to demonstrate adherence to Good Machine Learning Practices and to seek pre-authorization for anticipated modifications to adaptive AI systems through a Predetermined Change Control Plan. These measures reflect a growing expectation that AI-driven products will incorporate lifecycle governance and transparent risk-management practices.

In the financial sector, the Office of the Superintendent of Financial Institutions (OSFI) finalized Guideline E-23 on Model Risk Management in September 2025, with an effective date of May 1, 2027. The guideline expands traditional model risk frameworks to explicitly encompass AI and machine learning, mandating that federally regulated financial institutions adopt enterprise-wide systems for AI lifecycle governance, ongoing performance monitoring, and risk mitigation. Notably, agentic AI tools are to be treated as "models" subject to the full scope of model-risk obligations, creating uniform expectations across the banking, insurance, and pension sectors. As AI adoption accelerates, similar developments are expected from other professional and sectoral bodies, with the Canadian Securities Administrators expected to introduce disclosure requirements for publicly listed companies deploying AI in material business activities.

Organizations operating interprovincially face similar challenges to those subject to multiple sectoral rules: both must manage compliance across different regulatory bodies, terminology, expectations, and enforcement timelines. Therefore, we expect to see an approach of ensuring compliance and alignment with the highest applicable standards, whether they originate from a sectoral regulator, provincial legislation or a combination of both.

Looking ahead, as organizations continue to navigate the post-AIDA landscape, effective AI governance will require vigilance in 2026 by continuously monitoring provincial legislation, sector-specific regulatory guidance, and emerging international standards. In practice, this means adopting governance frameworks that accommodate provincial variation or align with the most stringent standards across the jurisdictions in which they operate.

For interprovincial organizations, harmonizing policies to the highest applicable provincial requirements, such as Québec's automated decision-making rules, offers both compliance certainty and a strategic advantage by demonstrating robust governance to regulators, courts, and stakeholders. Likewise, early alignment with international frameworks such as ISO/IEC 42001 and the NIST AI Risk Management Framework can streamline future compliance and reduce long-term implementation costs.

As organizations seek to ensure they are best positioned for success under this decentralized regulatory framework, we expect to see greater adoption of the highest standard across their organization where commercially reasonable, strengthening internal accountability and long-term readiness.

Trend #3: Cybersecurity and Data Management Will Demand More Formalized, Evidence-Based Governance as Regulatory Expectations Mature

Regulators worldwide are shifting from principles-based guidance toward prescriptive, auditable requirements for privacy, cybersecurity, and data governance. Courts and oversight bodies are also intensifying scrutiny of high-risk technologies and cross-border data practices. Below are the four trends we anticipate will be the most significant in 2026.

REGULATORY GOVERNANCE WILL DEMAND MOVEMENT TOWARD FORMAL, AUDITABLE PRIVACY AND CYBER GOVERNANCE

Regulators in multiple jurisdictions are moving decisively away from principles-based expectations and toward mandatory, reviewable, and fully documented compliance processes. Updated requirements for Privacy Impact Assessments (PIAs) now oblige institutions to complete a written PIA before collecting personal information, outlining mitigation measures and assessing security risks.[13] These changes elevate PIAs from discretionary exercises to enforceable obligations, creating new expectations for recordkeeping and auditability.

In parallel, regulators have demonstrated a willingness to block deployments of high-risk technologies, including a proposed supermarket facial recognition system, where organizations cannot show compliance with statutory standards.[14] Courts have also reaffirmed that privacy laws apply extraterritorially where a "sufficient connection" exists, expanding accountability for data collection conducted through online services.[15]

Technical Standards: De-Identification, Pseudonymization, and Identifiability Tests

Across key jurisdictions, regulators continue to emphasize repeatable technical standards over broad organizational discretion. Updated de-identification guidelines introduce checklists, step-by-step methodologies, and practical tools for managing structured datasets responsibly.[16] These materials signal a clear preference for standardized processes that can be monitored, tested, and demonstrated.

The Court of Justice of the European Union has likewise clarified that pseudonymized data remains personal data when a party can reasonably re-identify individuals.[17] This decision is in line with guidance that requires organizations to conduct and document realistic identifiability analyses grounded in actual re-identification capabilities rather than theoretical assumptions.[18]

13. Fasken's Noteworthy News: Privacy & Cybersecurity in Canada, the US and the EU (November 2025).
14. Fasken Noteworthy Privacy & Cybersecurity News (March 2025).
15. Fasken Noteworthy Privacy & Cybersecurity News (January 2025).
16. Fasken's Noteworthy News: Privacy & Cybersecurity in Canada, the US, and the EU (October 2025).
17. Pseudonymized Data: Key Takeaways from CJEU Decision.
18. Ibid.

Cross-Border Transfers and Embedded Operational Resilience

Courts continue to impose liability on organizations transferring personal data internationally without implementing appropriate safeguards, such as standard data-protection clauses or contractual clauses, underscoring that transfer governance must be supported by traceable, defensible documentation, rather than implied adequacy.[19]

Simultaneously, evolving regulatory expectations are embedding operational resilience requirements directly into privacy governance frameworks. Obligations relating to third-party risk management, concentration-risk evaluation, and contractual controls are becoming integral compliance elements.[20] Organizations are increasingly expected to incorporate auditable IT, cybersecurity, and vendor-management processes into daily operations to support regulatory transparency and strengthen overall resilience.[21]

SCRUTINY OF HIGH-RISK DATA COLLECTION & AUTOMATED DECISION TECHNOLOGIES WILL CONTINUE TO INTENSIFY

Necessity and Proportionality as Regulatory Baselines

Québec regulators continue to apply strict scrutiny to the use of biometric systems, requiring organizations to demonstrate necessity and proportionality before deploying any biometric solution.[22] Organizations must show that the purpose is legitimate, that less intrusive alternatives were assessed, and that biometrics are an appropriate and effective means of achieving the objective.[23]

In practice, this requires documenting the business need and rationale for using biometrics, including the problem being addressed and why alternatives were insufficient. Regulators have noted that organizations often fail to document these assessments adequately, reinforcing expectations for clear, recorded justification and disciplined decision-making when implementing biometric technologies.

Recent decisions to halt facial recognition pilots reflect the expectation that deployments satisfy proportionality requirements and legal-authority thresholds before implementation.[24] Enforcement pressure is especially rising in health contexts, with the first monetary penalties issued under provincial health-privacy legislation, signaling tangible consequences for inadequate governance and patient-data protections.[25]

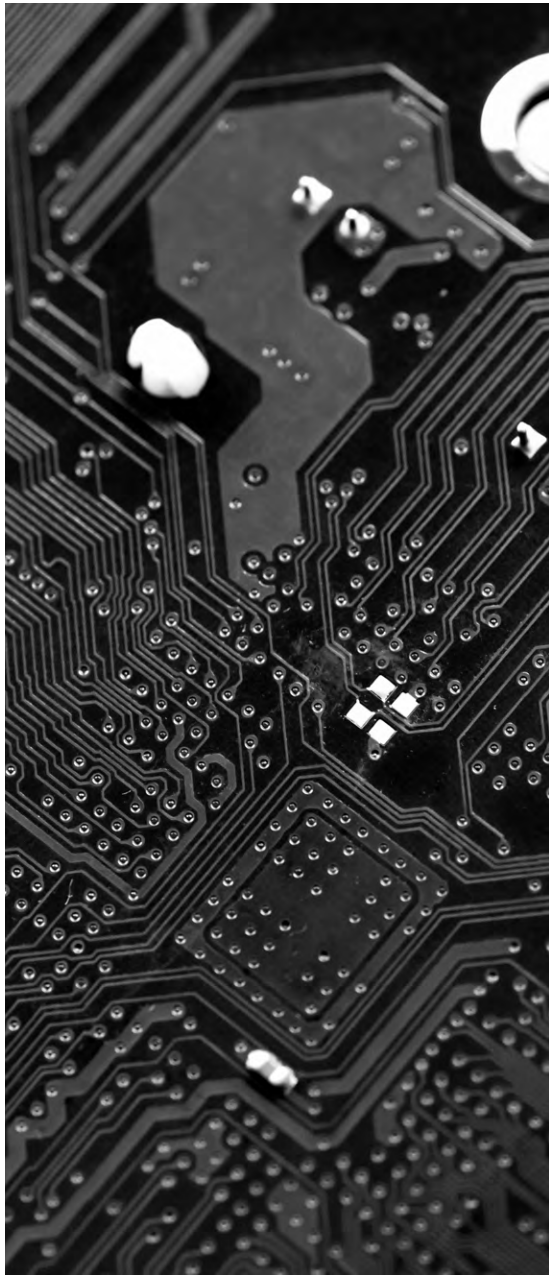
For high-risk data collection, regulators expect proof of necessity, plain-language transparency, consent where required, and audit-ready systems, underpinned by de-identification procedures and documented cross-border safeguards that can withstand scrutiny.

RISING CYBERSECURITY OBLIGATIONS FOR CRITICAL INFRASTRUCTURE

Mandatory Cybersecurity Duties for Essential Service Providers

Across jurisdictions, governments are placing sustained pressure on operators of critical infrastructure, including telecommunications, energy, finance, transportation, and health, to meet mandatory, enforceable cybersecurity standards. The progression of Bill C-8, which would enact the *Critical Cyber Systems Protection Act*, is a clear indicator of this shift. The framework introduces binding cybersecurity obligations for operators of federally regulated vital services and grants the federal government authority to issue legally enforceable cybersecurity directions and impose substantial penalties for non-compliance.[26]

19. Fasken Noteworthy Privacy & Cybersecurity News (January 2025).
20. A Series: Managing Legal Risk Associated with IT Outages Through Contracting Best Practices – Force Majeure.
21. Ibid.
22. Eight Tips to Smoothly Implement Your Biometric System.
23. Ibid.
24. Fasken Noteworthy Privacy & Cybersecurity News (March 2025).
25. First Monetary Penalties Issued under Ontario's Health Privacy Law: Practical Lessons for the Health Sector.
26. Bill C-8 Reboots Canada's Cybersecurity Legislation for the Telecommunications Sector and Other Critical Infrastructure.



This trend is reinforced by parallel enforcement in sensitive sectors such as health, where regulators have issued the first monetary penalties for inadequate safeguards, signaling a willingness to act when essential services fail to meet expected levels of protection.[27]

Internationally, this push is mirrored in the European Union through the Network and Information Security Directive 2 (NIS2), which broadens mandatory security and incident-reporting obligations and extends coverage to a larger set of "essential" and "important" sectors. NIS2 empowers authorities to issue binding instructions, conduct audits, and levy significant fines.[28]

Taken together, these developments illustrate a new regulatory view: cybersecurity is no longer a best practice but a legal duty for operators whose systems underpin public welfare or economic stability.

Rise of Prescriptive Frameworks and Incident Response Standards

Beyond raising expectations, regulators are introducing highly prescriptive frameworks that require organizations to formalize, operationalize, and evaluate their cyber-resilience capabilities. The EU *Digital Operational Resilience Act* (DORA) exemplifies this shift in the financial sector, mandating structured information and communication technology (ICT) risk-management processes, ongoing operational-resilience testing, rapid cyber-incident reporting, and rigorous third-party risk oversight for entities that play essential roles in the economy.[29]

Taken together, these measures reflect a sustained regulatory shift: cyber resilience for critical infrastructure is no longer voluntary or reactive. It is becoming a standardized, enforceable obligation grounded in mandatory controls, documented readiness, and assured incident-response capability.

NATIONAL & CROSS-BORDER COORDINATION ON CYBER AND DATA GOVERNANCE WILL CONTINUE TO BECOME COMMONPLACE

Convergence Toward Unified CyberResilience Standards Across Jurisdictions

Governments are adopting increasingly harmonized approaches to cybersecurity oversight, signaling a shift away from fragmented expectations and toward coordinated minimum baselines. NIS2 exemplifies this convergence by imposing standardized cybersecurity, governance, and incident-reporting duties across essential and important sectors in the European Union, supported by expanded supervisory powers such as audits and binding instructions.[30]

27. First Monetary Penalties Issued under Ontario's Health Privacy Law: Practical Lessons for the Health Sector.
28. European Union's NIS 2 Directive – What You Need to Know.
29. The Digital Operational Resilience Act (DORA) – How Will it Impact Canadian Businesses?
30. European Union's NIS 2 Directive – What You Need to Know.

Complementing NIS2, DORA establishes uniform digital-resilience expectations for financial entities operating within the EU, requiring structured ICT risk management, operational-resilience testing, and tiered incident-reporting protocols that apply consistently across ICT member states.[31]

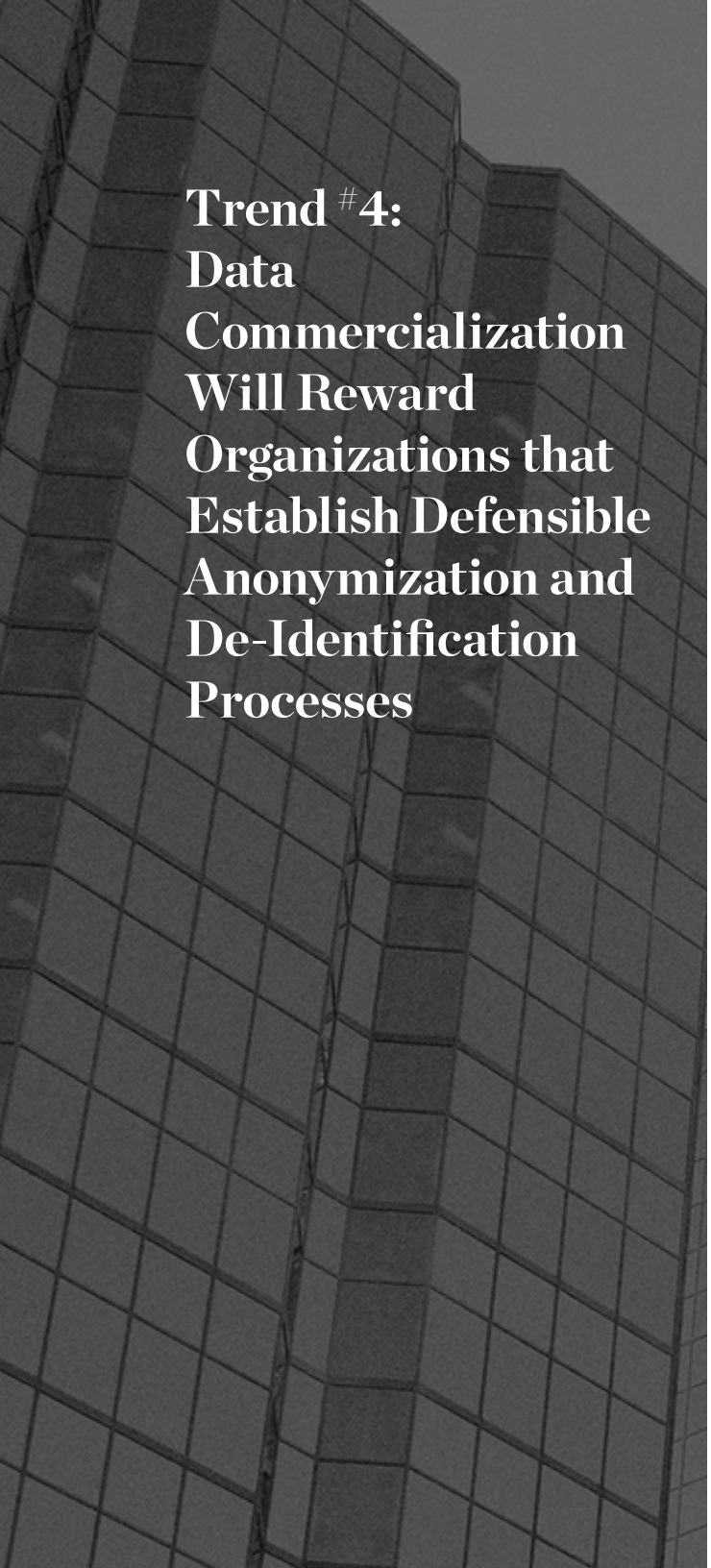
The repeated introduction of such frameworks across multiple regions indicates a shared international objective: strengthening baseline resilience for systems that support economic stability, national security, and essential public functions.

CrossBorder Data Governance and Regulatory Alignment

Growing coordination is equally evident in the evolution of data-governance measures, including updated approaches to cross-border transfers, consistent transparency expectations, and clearer standards for the handling of personal data. Courts and regulators continue to refine the legal tests governing international data flows, emphasizing the need for robust safeguards and formalized transfer analysis, an approach underscored by findings that indicate inadequately protected transfers outside the European Union.[32]

Taken together, these developments show that cybersecurity and data-governance expectations are increasingly stabilizing around shared international principles, reducing fragmentation and establishing a coordinated foundation for global digital resilience.

31. The Digital Operational Resilience Act (DORA) – How Will it Impact Canadian Businesses?
32. Fasken Noteworthy Privacy & Cybersecurity News (January 2025).



Trend #4: Data Commercialization Will Reward Organizations that Establish Defensible Anonymization and De-Identification Processes

We are well into the age of the cloud and big data, and to succeed, organizations must treat data as a strategic asset. Organizations across industries are working to organize their data into actionable insights and transform it into a source of strategic advantage. The pace of progress in AI requires that organizations be decisive in doing so. For organizations (and service providers in particular), the challenge is extracting economic value from data, including by using aggregated and anonymized data, while complying with laws and contractual obligations.

COMMERCIALIZATION OPPORTUNITIES

Organizations are finding new value in anonymized and aggregated data across financial services, healthcare, telecommunications, utilities, and consumer goods:

- **Financial Services – Personalized Products:** Insurers and brokers license aggregated behavioral data to tailor offerings and pricing.
- **Healthcare – Data Marketplaces & Partnerships:** Pharma, biotech, and AI-driven medical device firms acquire anonymized datasets for R&D and clinical trials, and to develop new devices and services.
- **Telecommunications – Network Optimization:** Aggregated usage data is used to optimize bandwidth, predict outages, and supports urban planning.
- **Utilities – Analytics and Compliance:** Energy providers partner with IoT firms to commercialize anonymized smart meter data for sustainability reporting and ESG compliance.
- **Retail and Consumer Goods – Targeted Marketing:** Anonymized demographic and behavioral insights drive advertising strategies; anonymized logistics data improves forecasting and cost efficiency.

Some verticals present particular regulatory challenges. Healthcare, for example, requires careful navigation of health-privacy laws. Even so, the global healthcare data-monetization market is projected to grow from $0.58B in 2025 to $1.16B by 2030, driven by real-time patient data, predictive analytics, and Data-as-a-Service (DaaS) models. Broader data-monetization markets are expected to reach $16.1B by 2033, driven by AI, cloud computing, and advanced analytics, with BFSI, telecom, and healthcare leading adoption.

TRENDS FOR DATA COMMERCIALIZATION

Observable trends in unlocking value and competitive advantage from data include:

Privacy-Enhancing Technologies for Data Sharing

Data clean rooms have transitioned to mainstream enterprise adoption. These secure computational environments allow organizations to collaborate on data analysis, for example, advertising attribution, retail partnerships, or financial services insights, without exposing personal or other sensitive information to counterparties. Major cloud providers now offer clean room solutions as standard enterprise offerings, and industry-specific clean room networks are emerging in sectors including healthcare and financial services.

Synthetic Data

Artificially generated datasets that preserve the statistical properties of source data without containing personal information – often referred to as "synthetic data" – have emerged as a significant commercial-product category. Organizations are both monetizing their proprietary datasets by selling synthetic derivatives and purchasing synthetic data for AI model training, software testing, and analytics development. Synthetic data offers a path to data commercialization that, when properly implemented, may avoid the application of certain privacy law requirements, though improperly anonymized or de-identified synthetic data may still be considered personal information under privacy laws.

AI Training Data

The AI and large language model boom have created increased demand for high-quality, licensed training data. Ongoing litigation and regulatory scrutiny around unauthorized use of copyrighted or personal information for AI training has made data provenance and clear licensing terms increasingly desirable.

First-Party Data Infrastructure

Tightening third-party cookie and mobile platform tracking restrictions have emphasized the importance of first-party data strategies for organizations that rely on digital advertising and customer analytics. Investments in customer data platforms, loyalty programs, and logged-in user experiences are some of the ways organizations are expanding their first-party data sources.

Data Cooperatives and Trusts

Data cooperatives and data trusts are structures where individuals or organizations pool data under arrangements that allow for the joint management of data provided by multiple stakeholders. These models are particularly relevant in sectors such as healthcare and agriculture, where individual data contributors have historically had limited ability to enter into such shared data arrangements.

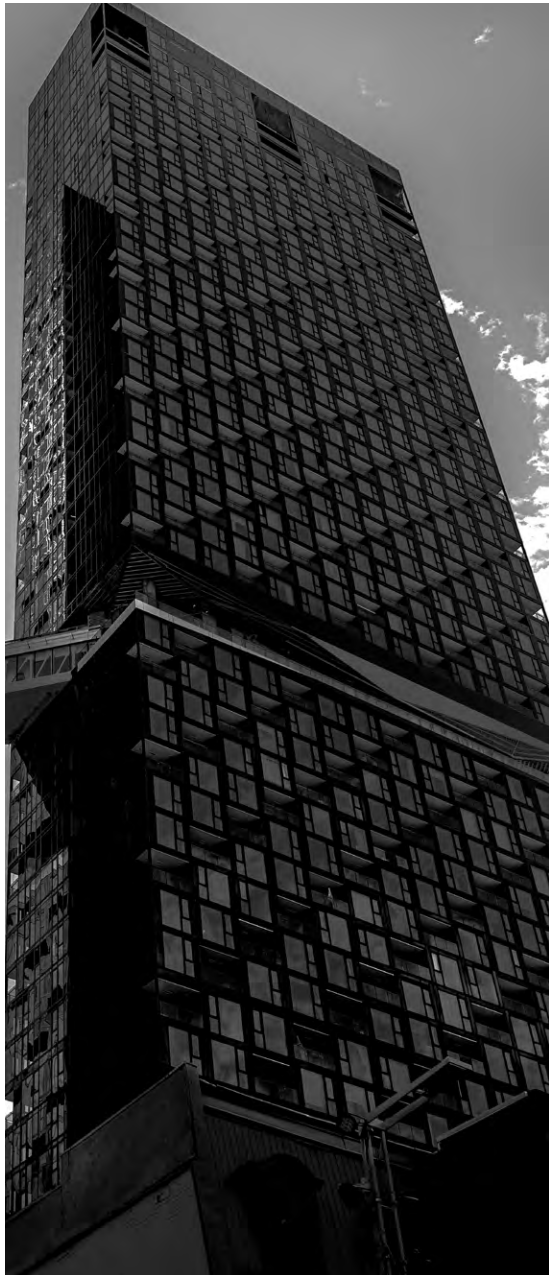
RISK & COMPLIANCE CHALLENGES

Data commercialization presents significant regulatory challenges. Certain privacy laws (particularly Québec's) have strict requirements surrounding anonymization. Advances in computing and external dataset availability have also increased re-identification risk. Laws outside of Canada also impose differing standards for anonymization and de-identification, creating compliance hurdles for multinational providers. Data breaches prior to anonymization can result in significant class action risks.

Ontario – De-identification Guidelines

The Information and Privacy Commissioner of Ontario (OIPC) updated and expanded its De-identification Guidelines for Structured Data on October 15, 2025, (Guidelines) replacing the 2016 version. The Guidelines frame de-identification as a practical, risk-based exercise aimed at reducing re-identification risk to a "very low" level, and emphasize balancing privacy protection with data utility to support legitimate secondary uses such as research, analytics, and innovation.

A central theme is that "context and controls" determine how risk should be assessed and managed. Public releases of de-identified information must assume adversarial access and therefore require more comprehensive transformations because enforceable controls on recipients are not possible, while non-public sharing of de-identified information can rely on contractual, privacy, and security controls to lower the probability of an attack on the de-identified information. The Guidelines set out a structured governance approach, including classifying direct vs. indirect identifiers, pseudonymizing direct identifiers, setting quantitative risk thresholds tied to privacy impact, measuring vulnerability, and calculating overall risk as vulnerability combined with probability of attack, supported by documentation and ongoing oversight. The Guidelines also stress that de-identification is not a single, one-time exercise, as risk assessments have limited shelf life and should be revisited periodically (often every two to three years) or when material changes occur, with monitoring for changing risk environments.



Québec – Anonymization Regulation

Where Québec personal information is involved, organizations must follow the *Regulation respecting the anonymization of personal information* (the Regulation), enacted under Québec's *Act respecting the protection of personal information in the private sector*. The Regulation sets out technical steps for anonymization, from initial planning to post-anonymization monitoring. Organizations must maintain a register recording a description of anonymized personal information, the purposes for using anonymized information, anonymization techniques and protection measures, and dates of re-identification risk analyses and updates.

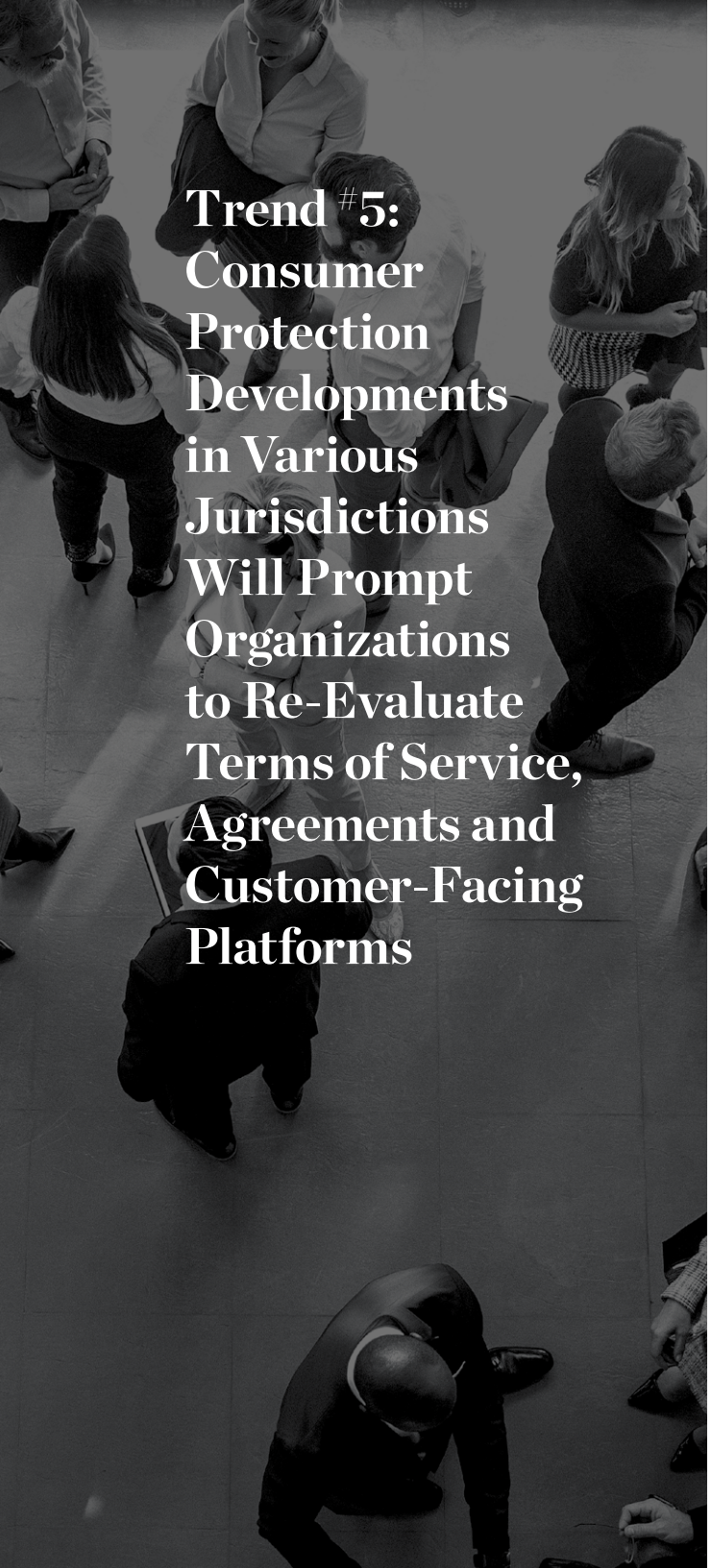
The Regulation requires organizations to conduct a preliminary re-identification risk analysis before anonymizing information, based on three core criteria. Correlation (whether records about the same person can be linked across datasets), individualization (whether a person can be isolated or distinguished within the dataset), and inference (whether personal information can be deduced from other available information). This analysis must also consider the broader context, including the possibility of linking with other reasonably available information, including public sources.

After applying anonymization measures, the organization must demonstrate that it is reasonable to foresee that the data can no longer identify a person (directly or indirectly) irreversibly, and that any residual re-identification risk is "very low"; the Regulation does not require proving zero risk. Whether risk is "very low" is assessed by considering factors such as the context and purpose of the anonymization, the nature of the data, the three criteria set out above (correlation, individualization, and inference), availability of other information, and the means and effort required to re-identify. The Regulation also expects periodic reassessment. If updated analysis no longer supports a very low residual risk, the dataset is no longer treated as anonymized.

Federal – Potential Privacy Reform

Bill C-27, the *Digital Charter Implementation Act, 2022*, died when Parliament was prorogued in January 2025. Bill C-27 included: (i) the *Consumer Privacy Protection Act* (CPPA), which would have replaced Part 1 of PIPEDA; (ii) the *Personal Information and Data Protection Tribunal Act* (PIDPTA), which would have established an administrative tribunal to hear appeals of Privacy Commissioner decisions and impose administrative monetary penalties; and (iii) the *Artificial Intelligence and Data Act* (AIDA).

Federal private-sector privacy reform is still expected, however, and any new legislation is anticipated to be similar to the CPPA and PIDPTA, although without AIDA. Organizations that rely on the anonymization of personal information should watch closely for the introduction of federal private-sector privacy reform in 2026.



Trend #5: Consumer Protection Developments in Various Jurisdictions Will Prompt Organizations to Re-Evaluate Terms of Service, Agreements and Customer-Facing Platforms

Canada's consumer protection landscape is undergoing significant reform. While the country's framework remains a patchwork of provincial and territorial statutes with federal overlays, recent legislative initiatives signal a potential shared momentum toward modernization and stronger consumer safeguards.

As more provinces update their statutes to reflect evolving market practices, national trends are beginning to emerge, creating both challenges and strategic opportunities for businesses operating in Canada. We expect that additional legislative and regulatory activity will accelerate this trend, introducing new compliance risks. Businesses should therefore anticipate further provincial regulatory harmonization and prepare for operational changes to consumer-facing e-commerce platforms. Below we outline the major trends that we have observed across jurisdictions and discuss what businesses should keep top of mind as Canadian consumer protection laws continue to evolve.

PROVINCIAL REFORMS PRODUCE NATIONAL TRENDS

Emphasis on Disclosure and Express Consent

A defining feature of recent legislation is the increasing demand for clarity and transparency in consumer contracts. Provinces are moving away from frameworks that allow contractual changes based solely on advance notice and are instead requiring express consent. For example, Ontario's ongoing consultations under the *Consumer Protection Act, 2023,* suggest that express consent will likely become mandatory for both amendments and continuations of consumer contracts, with draft proposals suggesting a consolidated set of "core" rules for most consumer agreements.

These changes signal a potential drift toward Québec's consumer model, which has long imposed robust requirements for informed consent and consumer autonomy.

Restrictions on Limiting Consumer Remedies

Another shared theme is the prohibition of certain contract terms, particularly those that restrict consumers' access to legal recourse and public expression.

In Ontario, for example, mandatory arbitration clauses and class action waivers are already prohibited under the existing *Consumer Protection Act, 2002*. The updated *Consumer Protection Act, 2023* (which is still not in force, despite receiving Royal Assent in late 2023) goes further by also prohibiting contract terms that prevent consumers from posting reviews, penalize them for negative feedback, or limit their ability to file complaints.

Similarly, in British Columbia, new amendments to its *Business Practices and Consumer Protection* Act would (once in force) align British Columbia law with Ontario and other Canadian jurisdictions by prohibiting: (i) mandatory arbitration clauses, (ii) class action waivers, and (iii) clauses that restrict online reviews or commentary.

These developments align with consumer-focused policy goals of improving marketplace fairness.

Regulation of Subscription and Auto-Renewal Models

Another key focus of consumer protection reforms is the regulation of subscription-based services and future performance agreements, particularly in the context of e-commerce.

In Ontario, the consultation process regarding the still-unreleased regulations to the (not-yet-in-force) *Consumer Protection Act, 2023* demonstrated a willingness to contemplate the following regulatory tools: (i) a "click-to-cancel" requirement for subscriptions and memberships, (ii) enhanced disclosure obligations for renewals and amendments, and (iii) a greater emphasis on express consent for changes and renewals.

In British Columbia, the aforementioned amendments to the *Business Practices and Consumer Protection Act* would: (i) render automatic renewals void unless consumers can cancel at any time, (ii) provide that cancellations must be penalty-free for renewals of 60 days or less, and require refunds or penalty-free cancellation for longer periods, and (iii) require suppliers to include prescribed disclosures and allow consumers to cancel for non-compliance.

Enforcement focus may therefore be shifting toward greater regulation of subscription and auto-renewal practices.

Rewards Points and Loyalty Programs

Loyalty programs remain an area of particular interest to consumer protection regulators. One of the new topics, for example, that New Brunswick's new *Consumer Protection Act* (finalized in 2024 but still not in force) will introduce to that province, is a regime to regulate loyalty programs. This will bring New Brunswick in line with other provinces, such as Ontario.

Ontario's omnibus Bill 46 (*Protect Ontario by Cutting Red Tape Act, 2025*) established a new framework for regulating loyalty programs under the current *Consumer Protection Act, 2002,* despite the existence of the still-not-yet-in-force *Consumer Protection Act, 2023*. Key features of this new framework include:

- Rewards points cannot expire, be cancelled, or suspended except as permitted by regulation;
- Consumers may request reinstatement of improperly expired or cancelled points; suppliers must comply or provide written reasons for refusal;
- Consumers are provided with a private right of action to recover disputed points; and
- Regulations are authorized to apply retroactively to agreements made before the law takes effect, creating significant compliance risk for existing loyalty programs.

Businesses offering loyalty programs should therefore review their program terms and prepare for potential retroactive enforcement once these new rules for loyalty programs are finalized and come into force.

Heightened Enforcement Powers

Recent legislative changes include increased fines, new administrative penalties, and expanded consumer access to tribunals. For example, Ontario has proposed increasing fines for consumer-protection contraventions to up to $100,000 for individuals and $500,000 for corporations. British Columbia, meanwhile, has expanded its Civil Resolution Tribunal's jurisdiction for claims under $5,000.

These changes demonstrate a trend away from education-based compliance (e.g., guidance letters, informal warnings, or collaborative outreach aimed at resolving non-compliance) and toward more aggressive regulatory enforcement (e.g., administrative monetary penalties, higher maximum fines, private rights of action, and tribunal-awarded damages for statutory breaches).

Practical Implications: What Businesses Should Do Now

While many of these laws are not yet in force and key regulatory details remain pending, a clear national direction is emerging. There are proactive steps that businesses can take now to prepare for these changes.

- Review consumer-facing contracts and policies for compliance with evolving requirements (e.g., cancellation rights, subscription renewals, disclosure obligations).
- Understand the risk of including prohibited terms, especially those restricting legal recourse (e.g., arbitration clauses), consumer feedback, or class proceedings.
- Tailor consumer agreements to specific provincial regimes where appropriate. A "one-size-fits-all" national contract (with carveouts for only Québec) may no longer be sufficient given the diverging scope and timing of provincial reforms.
- Prepare for greater scrutiny and enforcement, including the potential for retroactive challenges.
- Monitor regulatory consultations and pending regulations, particularly in jurisdictions such as Ontario and New Brunswick, where much of the operational rules remain in draft form (or is nonexistent).
- Audit loyalty and rewards programs for compliance with Ontario's new rules and potential retroactive obligations.
- Prepare for retroactive enforcement risks by reviewing legacy agreements.

Canadian consumer protection law is entering a new era, with a degree of national alignment around key principles of fairness and, transparency. Moreover, if economic challenges continue for consumers into 2026, it would not be surprising to see consumers asking more from their elected officials and regulators in connection with consumer protection. At the same time, there is an observable trend of consumer protection changes being introduced by legislatures but never taking effect.

As these reforms continue to take shape, companies operating or supplying consumer goods or services in Canada should have legal counsel review their existing business-to-customer agreements and customer-facing platforms. Understanding and anticipating these national trends will be critical for maintaining legal compliance, protecting reputational value, and delivering a consistent customer experience across Canadian jurisdictions.

Trend #6: Fintech Will Enter a Pivotal Year as the Retail Payment Activities Act Supervisory Controls and Real-Time Rail Reshape Canada's Payments Ecosystem

Canada's Real-Time Rail (RTR) system, led by Payments Canada, is positioned to fundamentally modernize the country's payment infrastructure by delivering real-time, always-on, data-rich payments. Two major developments in 2025 have set the stage for this transformation. First, Payments Canada expanded membership eligibility by implementing amendments to the *Canadian Payments Act* (CPA) that allow registered Payment Service Providers (PSP) to apply for direct participation in RTR, rather than relying on a connection service provider. Second, the Bank of Canada began supervising nearly 1,500 PSPs under the *Retail Payment Activities Act* (RPAA) in preparation for allowing PSPs direct access to the RTR system.

For financial institutions, these changes are more than operational, signaling a shift toward an open, competitive payments ecosystem. RTR will clear and settle payments within seconds, providing immediate confirmation and reducing systemic friction. Looking ahead, the government's plan to legislate "write access" by mid-2027 will further accelerate innovation, enabling accredited third parties to directly initiate actions such as account switching and payment initiation. This evolution introduces both opportunity and complexity. Institutions that participate must navigate new compliance obligations, assess strategic participation models, and prepare for heightened regulatory scrutiny, all while positioning themselves to leverage RTR's potential for efficiency and customer-centric innovation.

THE RPAA: MOVING TO ACTIVE SUPERVISION

The RTR ecosystem rests on two complementary legislative pillars, the first being the CPA, which governs interoperability and system-level safety for clearing and settlement systems. The second is the RPAA, which establishes risk and security standards for PSPs at the entity level. Both Acts involve oversight by the Minister of Finance and the Bank of Canada, but with distinct objectives: system stability for the CPA and retail payment activity for the RPAA.

The RPAA established a new supervisory framework for PSPs when core compliance requirements took effect on September 8, 2025.[33] In 2026, the Bank of Canada will move from issuing guidance to actively evaluating how well PSPs are meeting their obligations, marking a shift in focus from implementation to assessment, including a requirement for annual reports.[34]

---

33. Bank of Canada - Supervisory framework: Supervision.
34. Annual reports are due each year on March 31, with submissions requiring up-to-date registration information and information about operational risk management, incident response and safeguarding practices for end-user funds.
The Bank of Canada will use these submissions to assess how PSPs are managing emerging risks and to identify where supervisory attention is warranted: Bank of Canada - Supervisory framework: Supervision. See also Bank of Canada - Administrative monetary penalties

SETTING THE SUPERVISORY TONE

The Bank of Canada's response to the first wave of annual reports may establish supervisory baselines and expectations. We expect that PSPs with established effective safeguarding frameworks, maintained comprehensive incident logs, and demonstrated board-level oversight will be more likely to proceed with minimal supervisory engagement. Conversely, PSPs with gaps in safeguarding controls, incomplete incident documentation, or inadequate third-party oversight may signal to the regulator that increased supervisory examination or enforcement activity may be warranted.

Notably, the Bank of Canada can impose administrative monetary penalties up to $1 million for serious violations and up to $10 million for very serious violations. Furthermore, repeated non-compliance with reporting requirements or supervisory expectations can result in registration revocation. We expect that organizations will be more alert to this year's reporting obligations as they navigate the new supervisory framework, which will likely require comprehensive reviews of compliance documentation to ensure all components are complete and accurate.[35] The Bank of Canada's enforcement decisions in early 2026 may signal which categories of compliance failures it views as most significant as well as provide practical guidance on regulatory priorities and enforcement tolerance.

THE IMPLEMENTATION PATHWAY

The defining legal feature of the RTR is the finality of settlement. Once a payment settles, which occurs within approximately 10 seconds, it generally cannot be reversed or recalled. This differs fundamentally from the current Automated Clearing Settlement System (ACSS) environment, where payments may be returned in various circumstances. Under the RTR framework, payments may only be returned in three situations: errors, unauthorized payments, and fraud. When a receiving institution receives a return request for fraud, it must respond to the request within 10 calendar days.[36]

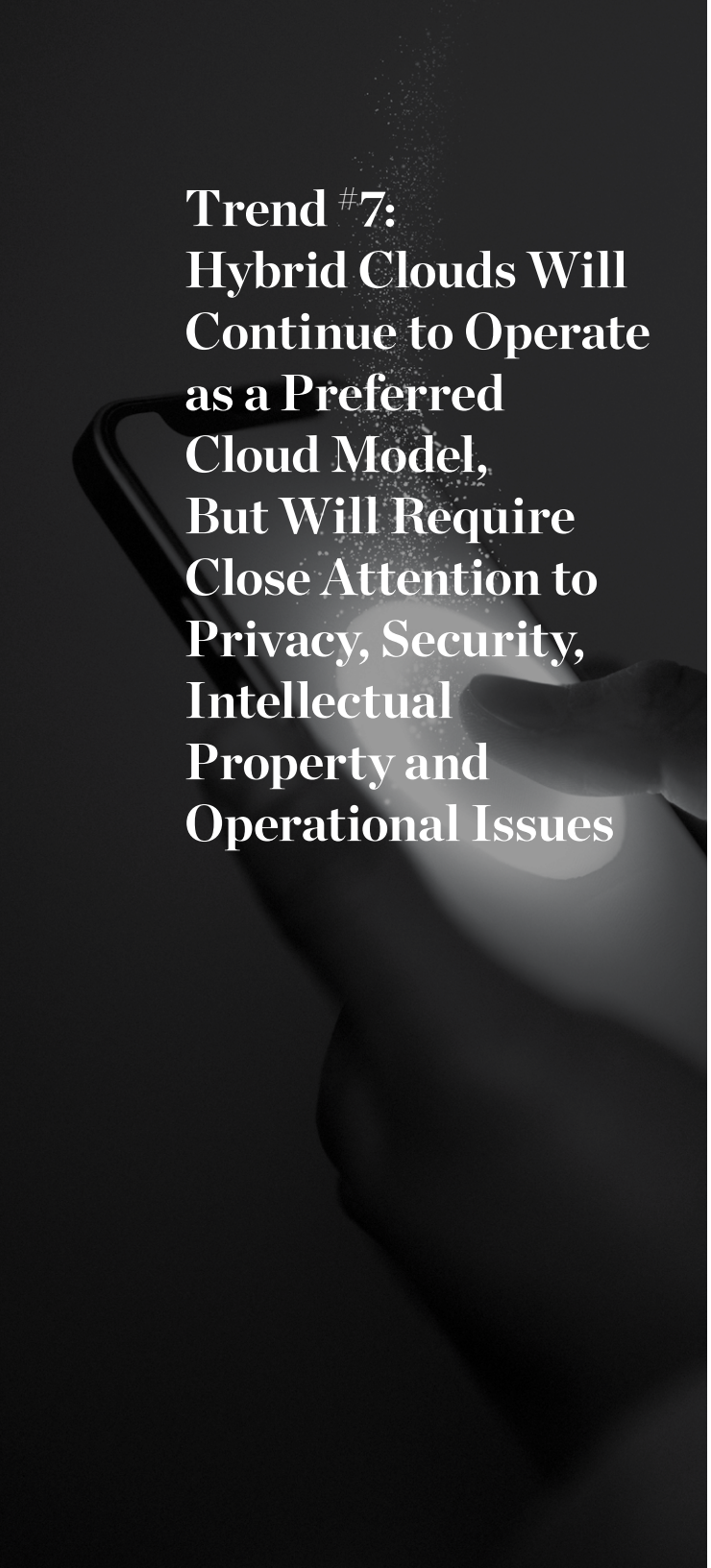
This settlement architecture creates a different operational and legal environment for PSPs in which the window for intervention becomes compressed and demands greater proactivity for fraud risk management. Given this reality, Payments Canada has implemented a centralized fraud prevention infrastructure for RTR participants. This includes mandatory incident reporting to ensure participants share information about flagged accounts and access fraud signals prior to settlement. Participants must also implement multi-factor authentication and establish procedures to investigate and respond to fraud indicators. Failure to maintain compliance with these fraud prevention requirements may result in temporary restrictions on RTR access.[37]

Over the course of 2026, PSPs should consult with their third-party service providers to confirm proper understanding of the fraud prevention framework and the associated allocation of responsibilities for fraud investigation. Pre-payment verification mechanisms will likely become essential controls, and it will be critical that legal and technology teams ensure that confirmation of payee and other fraud prevention capabilities are fully operational and integrated into payment processes.

ORGANIZATIONAL PREPARATION FOR 2026

2026 will be a pivotal year for Canadian payments regulation, marked by the rollout of the RPAA supervisory controls and the implementation of RTR. Early enforcement actions by the Bank of Canada will set supervisory expectations and highlight critical compliance priorities for PSPs. As competitive dynamics shift with broader access to Payments Canada membership, financial institutions should proactively review pricing, partnerships, and compliance strategies. Those within an organization who prepare RPAA documentation, evaluate RTR participation, update customer agreements, and track regulatory guidance will play a vital role. By updating operational procedures and ensuring readiness for real-time, irrevocable payments, organizations will be well-positioned to navigate the evolving regulatory landscape in 2026.

35. Bank of Canada - Enforcement tools
36. Payments Canada - RTR Participation Guide Payment Service Providers
37. Payments Canada - Real-Time Rail public consultation reconfirms strong industry support for Canadian real-time payment system



Trend #7: Hybrid Clouds Will Continue to Operate as a Preferred Cloud Model, But Will Require Close Attention to Privacy, Security, Intellectual Property and Operational Issues

Hybrid cloud, an architecture that blends public cloud services with private cloud or on-premises infrastructure, has moved beyond buzzword status to become a preferred cloud operating model for many technology-forward organizations. Gartner, for example, predicts that 90% of organizations will adopt hybrid cloud by 2027, driven by AI workloads and multicloud strategies.[38]

The drivers behind such an approach are practical: hybrid clouds allow enterprises to maintain control over sensitive workloads and the ability to modernize legacy systems without a painful mass migration, while still being able to leverage classic cloud benefits such as elastic compute for variable demand, cost optimizations, and simplification of data backup and disaster recovery processes by using redundant cloud resources.

For Canadian organizations, particularly those in regulated sectors such as financial services, healthcare, telecom and the broader public sector, as well as others with data sensitivity concerns, the hybrid cloud approach also offers a way to navigate data residency and access expectations, as well as bespoke security requirements.

As adoption of hybrid clouds accelerates, organizations should, in parallel with implementing such infrastructure, adopt a strategic legal program that reflects the unique risk profile of such technology. Below, we outline certain key legal and regulatory issues that organizations should consider in developing such a program.

DATA RESIDENCY, PRIVACY AND CROSS-BORDER TRANSFERS

Hybrid clouds often split workloads, with sensitive data and mission-critical applications remaining on-premises or in private clouds, while less sensitive operations use the public cloud.

For Canadian organizations that deal with personal information, how to best leverage such a design should include consideration of Canadian privacy laws. For example, the federal private sector privacy legislation (PIPEDA), and the substantially similar provincial laws in Alberta, British Columbia and Québec, impose some level of requirements on cross-border transfers of personal information. Similarly, public sector statutes in British Columbia and Nova Scotia contain residency rules and constraints on the storage of identifiable personal information outside of Canada. Compliance with these regimes may therefore look different for private vs. public clouds.

38. CIO Dive - Global cloud spend to surpass $700B in 2025 as hybrid adoption spreads: Gartner (November 19, 2024)

Organizations may be able to reduce their privacy law compliance burden and mitigate certain data protection risks by ensuring that personal information and other sensitive data remain in a private cloud (assuming that such information can be isolated). As a result, contractual clauses with cloud vendors will need to clearly manage such risks, including restrictions on cross-border transfers. For example, many hybrid clouds include automated data burst policies that automatically transition data to the public cloud when on-premises capacity reaches specified thresholds. Practices like this may require new restraints. As a further example, in some cases, organizations may want to restrict public cloud processing to non-identifiable or de-identified analytics.

SECURITY AND SHARED RESPONSIBILITY

Traditional cloud configurations emphasize "shared responsibility models", whereby each of the cloud vendor and the customer assume distinct security responsibilities. Hybrid cloud intensifies that paradigm. Security obligations shift depending on whether the workload is on-premises/private cloud (often the customer's responsibility), or public cloud (often the vendor's responsibility or shared with the vendor). Organizations should be careful not to under-specify these distinctions in their contracts. Further, responsibility for security at the interface between public and private infrastructure is often unclear when relying on traditional cloud shared responsibility models. As a result, clear assignment of obligations will be key and traditional RACI charts may need to be expanded with greater detail in order to avoid an accountability gap.

Security related issues specific to the public-private cloud distinction should also be considered and addressed. The extent of security provided by the public cloud vendor, and the associated level of vendor accountability, may impact the data that needs to be restricted to the private cloud. Encryption of data in transit between public and private clouds may also be critical.

PERFORMANCE AND OPERATIONAL MANAGEMENT

Standard cloud contracts often presume a homogenous public cloud deployment and therefore may not reflect a performance and operational management model appropriate for a hybrid cloud. Organizations will need to take special care to ensure that performance and operational management provisions are updated to meet hybrid needs, including the following:

- **Service Levels**: Availability will continue to be a core service level metric in hybrid clouds. Commitments, however, should reflect end-to-end dependencies across private and public segments. Contracts should also define service level commitments for the hybrid connection and not just for individual infrastructure components. Otherwise, organizations may discover that an outage in one segment is not covered.
- **Change Management**: Traditional clouds often push evergreen changes simultaneously to the entire system. This may not be possible in a hybrid environment given the interplay between the public vs. private system components. Contracts may therefore need to contemplate protections such as planned update windows, advance notice of changes, and compatibility testing rights to manage these risks. As a further consideration, changes in one system may require corresponding updates in another system. Contractual obligations should be established to ensure ongoing compatibility. In this regard, traditional change order procedures may not be sufficient absent proper provisions for "mandatory changes".
- **Coordination**: As private and public clouds may be separately operated (either by multiple vendors or by a combination of the customer and vendors), vendor contracts may need to more expressly contemplate integration between systems as well as formal cooperation obligations among all relevant parties.

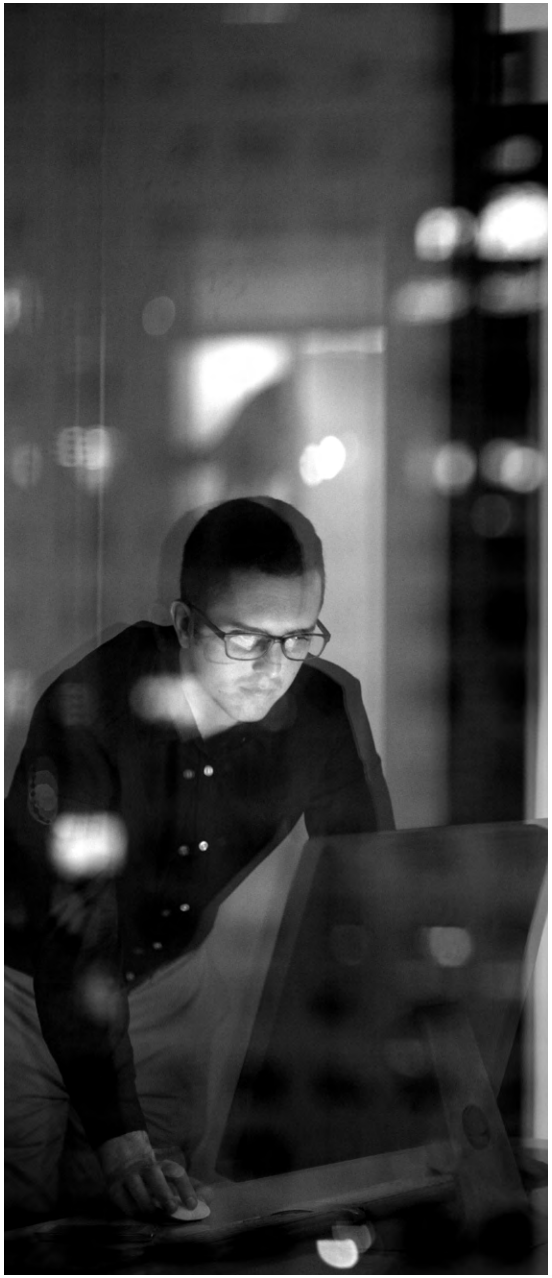
INCIDENT RESPONSE AND BREACH NOTIFICATION

In a hybrid cloud, incidents rarely respect boundaries. For example, a credential compromise in the public cloud could unlock private infrastructure, or a misconfiguration in the private cloud may expose data to public cloud infrastructure. Contracts should therefore ensure that breach investigation obligations consider potential cross-contamination issues between public and private clouds. Notification obligations should, for example, consider whether a breach in the public cloud results in a risk of harm with respect to data in the private cloud such that disclosure requirements are triggered (e.g. under applicable privacy law). While a properly architected and configured hybrid system should prevent this from being an issue in theory, having contractual obligations to validate any practical risk will support compliance with legal obligations. A similar analysis may be appropriate in respect of regulatory obligations for Canadian financial institutions under OSFI Guideline B-13 or similar regulatory requirements in other regulated industries. A level of coordination among private cloud vendors and public cloud vendors may also be required for other elements of the incident response, including containment and remediation.

INTELLECTUAL PROPERTY

Hybrid clouds often require software code that integrates various components of the system. Contracts should therefore clarify applicable ownership and license rights. For example, integration code may reflect confidential information about the customer's business, or may provide the customer with a competitive advantage, in which case ownership of the code by the customer (or an exclusive license) will be important. Additionally, in the case of licensed code, traditional license restrictions prohibiting disclosure to and/or use by third parties may no longer be appropriate in a hybrid cloud, as those restrictions may hinder the required level of integration.

To conclude, hybrid clouds are proving to be popular, as they combine the traditional benefits of cloud computing, such as scalability and cost efficiency, with the traditional benefits of private infrastructure, such as control and security. Combining these models, however, raises unique challenges. Close attention must therefore be paid to the legal framework supporting hybrid clouds, including a particular focus on issues related to data privacy, security and shared responsibility, performance and operational management, incident response and breach notification, and intellectual property rights.



Trend #8: Complex and Strategic Deals will Drive Technology M&A, with AI Businesses Continuing to Fuel Activity

As was the case in 2025, Canada's technology sector is expected to remain a significant driver of M&A activity throughout 2026. In light of the headwinds in North American and global deals, tech M&A in 2025 could be described as disciplined. We observed a reduction in the number of transactions between 2024 and 2025 but this was balanced by an increase in aggregate deal value.[39] This trend reflected a concentration by buyers on higher-confidence opportunities with a clearer strategic rationale; buyers were cautious with capital but pursued deals perceived as high-quality. These deal dynamics of 2025 inform our reporting on four defining Canadian tech M&A trends that we anticipate will continue into 2026: the shift to fewer but larger and more strategic deals; continued focus on AI and software; adjustments to regulatory scrutiny; and expanded use of ancillary deal terms such as earnouts.

FEWER, BIGGER, MORE STRATEGIC TECH DEALS

The first defining trend in 2025 was the shift from a broad base of tech-deal volume to fewer, larger, more strategic transactions.[40] We anticipate that this pattern will persist into 2026. In technology and tech-adjacent sectors, this translates to a focus on acquiring assets that deliver durable cash flows and improved competitive positions, such as the acquisition of mission-critical SaaS providers, data-rich platforms and digital infrastructure. We have seen a decrease in speculative bets on early-stage innovation. This shift also reflects Canadian buyers' response to the practical business and macroeconomic realities of 2025, including geopolitical uncertainty and rapid digital transformation, which increased risks to deal completion. As companies continue to operate under similar conditions to begin 2026, we expect that Canadian tech M&A will remain active but skew toward targets that can demonstrate scale, recurring revenue and strategic fit in a more disciplined market.

39. MNP - Technology Quarterly Update Q3 2025
40. Ibid

AI REMAINS AT THE CENTRE OF CANADIAN TECH M&A DEAL FLOW

In our 2025 report, we anticipated that AI and related businesses would be highly sought-after assets as buyers raced to integrate AI capabilities and related infrastructure. Confirming our expectations, quarterly reporting by MNP[41] and PitchBook[42] in 2025 showed that Canadian tech transactions remained resilient despite geopolitical headwinds, with continuing demand for AI-driven software, cloud services and digital infrastructure. However, it remains to be seen whether the overwhelming growth in AI enthusiasm over the last few years will continue throughout 2026 as valuations reach potentially unsustainable levels and market sentiment continues to shift. As we move into 2026, we expect AI to remain a central theme in Canadian deal flow with Canadian AI-enabled software, analytics and cybersecurity companies remaining priority targets with valuations being increasingly based on more demonstrable and scalable use cases, reliable customer bases and verifiable revenue quality rather than simply "AI" branding or growth projections.

REGULATORY COMPLEXITY AS A TRANSACTION DETERMINANT

The Government of Canada's March 5, 2025 update to *Investment Canada Act* guidelines expanded national security review criteria to explicitly encompass "economic security" considerations, extending the focus beyond traditional defence and security concerns to include key elements of the Canadian innovation ecosystem.[43] The guidance highlights technologies on the Sensitive Technology List such as AI,[44] data storage and cyber security technology and signals the potential for increased regulatory scrutiny, which may extend timelines for transactions in the space. These practical implications will continue to be considerations for targets and acquirers throughout 2026.

It is important to note, however, that despite trade tensions and foreign investment sensitivities becoming practical constraints in technology transactions, cross-border activity continues to be an important part of the Canadian tech and broader M&A landscape. Many 2025 transactions involved international elements, whether they involved foreign buyers targeting Canadian companies or Canadian bidders seeking assets outside of Canada in sectors such as energy transition, critical minerals, and digital infrastructure that increasingly rely on sophisticated technology.

Competition law has also played an increasingly important regulatory role in AI transactions. While we have not yet seen this in a notable manner in Canada, international regulators, including the Federal Trade Commission and Department of Justice in the US and the UK's Competition and Markets Authority, are scrutinizing so-called "pseudo-mergers" in which large technology firms replicate the economic and competitive effects of an acquisition by acquiring exclusive IP rights, compute resources, and/or key tech talent. In contrast with more traditional, formal acquisitions these firms are not acquiring all, or substantially all of the assets of the target in a pseudo-merger. This occurred in a number of AI industry transactions in 2025.

M&A transactions are subject to regulatory review, but it is not clear if a more limited acquisition would trigger review in Canada. The federal *Competition Act* defines "merger" broadly and includes an express anti-avoidance rule permitting the Competition Bureau to look past legal form to the substance of a transaction. As a result, these structures may attract scrutiny where they foreclose competition or entrench incumbent market power, even if they fall below notification thresholds. The trend toward these transactions has not diminished in Silicon Valley and may continue into 2026 and potentially in the Canadian market. Acquirers and targets alike will need to carefully consider deal architecture, clear pro-competitive rationales, and early competition law assessment when structuring AI partnerships, talent acquisitions, or strategic alliances.

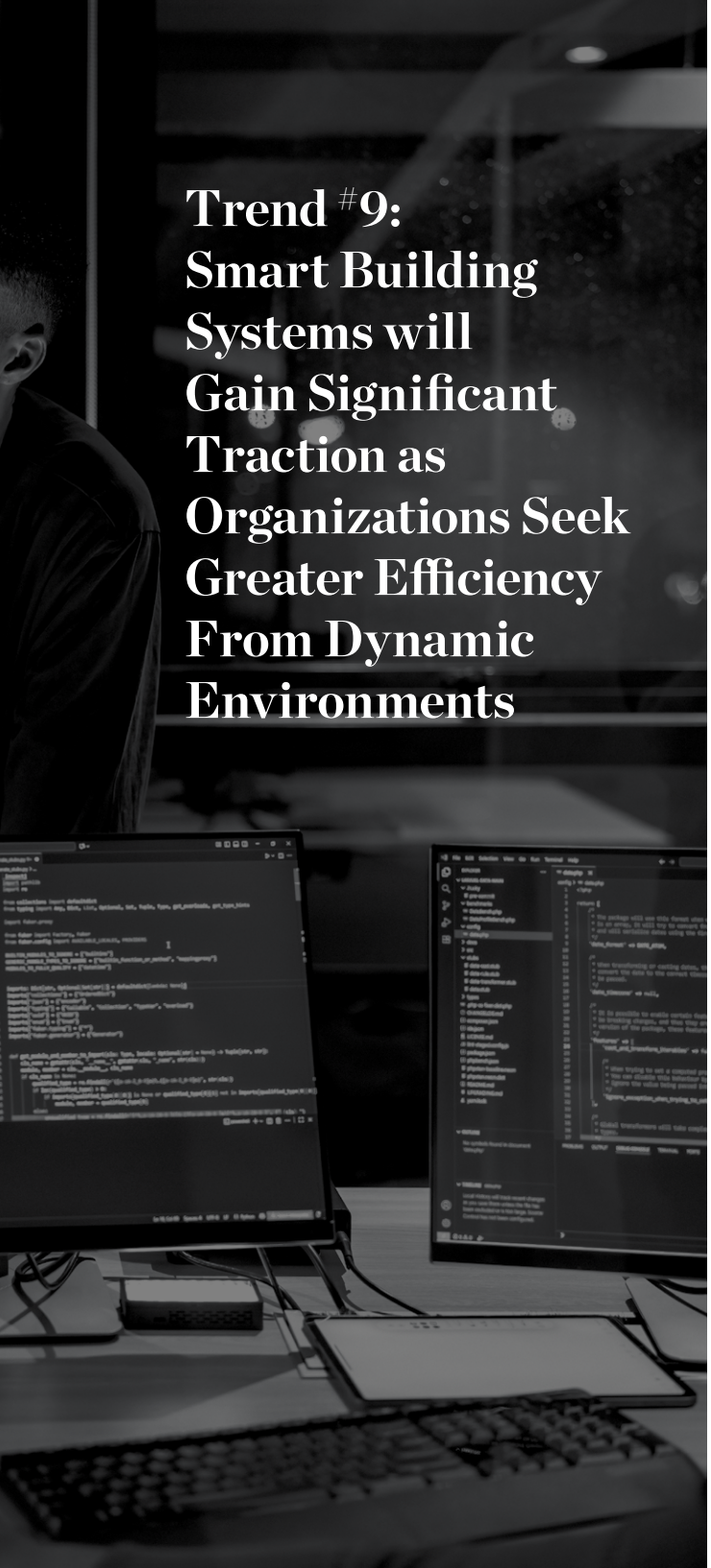
41. Ibid.
42. Data in this analysis is sourced from PitchBook, reflecting M&A and change of control transactions in Canada within the information technology sector for 2025.
43. https://ised-isde.canada.ca/site/investment-canada-act/en/updated-guidelines-national-security-review-investments
44. Canada's Sensitive Technology List identifies eleven broad technology areas that the Government of Canada considers to be sensitive. The technology areas in this list capture key areas with national security implications: https://www.canada.ca/en/services/defence/nationalsecurity/sensitive-technology-list.html

STRUCTURING AROUND VALUATION GAPS

A final trend in 2025 was the expanded use of deal-structuring mechanisms and contingent consideration arrangements to address valuation gaps, particularly in technology where future performance is difficult to predict. This included, most commonly, earnouts tied to revenue growth, customer retention, and technology specific operating metrics such as subscription churn or AI feature adoption. We expect continued reliance on these tools in 2026, meaning sophisticated parties will remain focused on precise drafting around performance metrics, operational control and dispute resolution mechanisms.[45]

With Canadian dealmaker confidence returning, the overarching message is that tech M&A in Canada remains in a disciplined phase: transactions will occur, but selectively. Tech M&A we will see strong but focused demand in 2026, with buyers targeting strategic Canadian assets that offer scale, resilient earnings, and credible AI or data-driven value propositions. Technologies such as AI, cybersecurity, cloud, and digital infrastructure, will likely continue to anchor deal flow, but parties should plan for heightened regulatory scrutiny, especially in transactions involving technology on, or adjacent to, the federal government's Sensitive Technology List. Finally, negotiations are likely to feature increased use of earnouts and risk-sharing mechanisms over purely fixed-price structures.

45. Lexpert - Weathering tech sector deal-making amid a global trade war.



Trend #9: Smart Building Systems will Gain Significant Traction as Organizations Seek Greater Efficiency From Dynamic Environments

The post-pandemic return to the office, and renewed support for large-scale infrastructure projects, have put the built environment back into the spotlight. As organizations re-imagine physical spaces, smart building technologies are central to creating environments that are adaptive, efficient, sustainable and data-driven. Yet, with innovation comes complexity. Developers, owners, and tenants must navigate a host of important legal considerations.

Smart buildings integrate systems such as HVAC, lighting, access control and energy management, into a connected ecosystem that can respond autonomously to environmental and human inputs. This involves a host of sensors to collect data, and systems to organize and present it for human or automated decision-making. Examples range from facial recognition access controls and climate systems that adjust to occupancy or weather, to cleaning robots, connected rodent traps, microbial sensors, and augmented reality tools for facility maintenance staff.

Enabled by the Internet of Things, AI, and big data analytics, smart buildings are not passive spaces but dynamic environments that learn, adapt, and optimize. While technologies vary from one smart building to another, even a single smart feature can raise important legal questions. As adoption accelerates and smart building technologies mature, developers, owners and users of these technologies must not lose sight of the risks, mitigation strategies, and responsibilities that accompany smart infrastructure. This requires considerations at both the data and system level as well as the commercial level.

DATA PRIVACY: GOVERNANCE AND OWNERSHIP

Smart buildings generate vast amounts of data, from occupancy patterns and energy usage to biometric inputs and environmental conditions. While data is essential to smart building systems, the volume and potential sensitivity raises significant privacy and data governance concerns.

In Canada, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs how private-sector organizations collect, use, and disclose personal information. Alberta, British Columbia, and Québec have their own substantially similar privacy laws.

Where data is identifiable to individuals, key legal obligations include:

- **Consent and transparency**: Organizations must obtain meaningful consent for the collection and use of personal information. They must clearly explain the nature and purpose of that collection and use, especially where sensitive data (such as biometric or location information) is involved. Guidance from the Office of the Privacy Commissioner of Canada on the use of facial recognition and video surveillance emphasizes the need for transparency, proportionality, and safeguards against misuse.

- **Data ownership and control**: Contracts with system providers must clearly define who owns and controls the data generated by smart building systems. This includes specifying rights to access, use, share, and monetize the data.
- **Safeguards**: Contracts with system providers should specify safeguards beyond generic requirements. Organizations must protect personal information according to its sensitivity, and data that is linked to identifiable individuals who live or work within the building must be subject to heightened safeguards.

Systems involving biometrics, such as those used to control access to premises, require additional scrutiny and caution. In Québec, such systems may trigger registration requirements and, in all jurisdictions, must undergo a privacy impact assessment, with mitigation measures implemented before deployment.

CYBERSECURITY AND SYSTEM INTEGRITY.

The interconnected nature of smart buildings creates significant exposure to cyber threats. A single compromised IoT device can compromise the entire system, exposing sensitive data and disrupting operations.

In Canada, PIPEDA requires organizations to report privacy breaches involving a "real risk of significant harm" to affected individuals and to the Privacy Commissioner of Canada. Organizations must also maintain records of all breaches. Similar obligations exist under some provincial privacy laws.

Organizations that rely on smart building systems should take special care to implement layered security protocols and breach response plans, with a view to effectively preventing, detecting and responding to cybersecurity incidents. Disaster recovery and business continuity plans must address unique scenarios where system failures render premises inaccessible. Contracts with vendors and service-providers include clear cybersecurity standards and breach response requirements.

Government agencies and standards-producing organizations have already started to publish administrative guidance on how to ensure the security of these emerging technology systems. For example, the Canadian Centre for Cyber Security's July 2025 publication, *Security considerations for critical infrastructure (ITSAP.10.100)* provides recommendations for securing IoT systems and critical infrastructure. Organizations should look to this guidance for best practices and other measures to incorporate into contracts for smart building systems and services.

CONTRACTUAL STRUCTURES AND RISK ALLOCATION.

Smart building projects involve multiple stakeholders, including developers, owners, technology providers, contractors, and tenants. Clear contractual frameworks are critical to avoid blurred roles and responsibilities and to allocate responsibilities and risk across those stakeholders.

Depending on an organization's role, key issues include:

- **System failures**: Contracts should address liability for malfunctions, downtime, and performance shortfalls, including maintenance obligations and remedies.
- **Technology upgrades**: Given the shorter lifecycle of software compared to physical infrastructure, contracts should address upgrade paths, compatibility requirements, and associated costs.
- **Commissioning and testing**: Contracts should include protocols for system testing and acceptance (including in relation to upgrades) to prevent disputes and ensure performance standards are met.

Smart buildings sit at the intersection of real estate, technology, and data. As smart buildings become common in workplaces, public facilities and residential complexes, proactive legal strategies will be key to unlocking their full potential while mitigating risk. Organizations that plan for these issues early, during procurement, design, and commissioning, will be better positioned to mitigate risk, meet regulatory expectations, and fully leverage the benefits of connected infrastructure.

Trend #10: Digital Sovereignty Will Depend On Execution, Not Aspiration, As Organizations Seek To Demonstrate Tangible Outcomes From Investments

In 2025, Canada placed digital sovereignty at the centre of its technology strategy. Digital sovereignty is no longer a theoretical concept and has evolved into a practical response to the growing need for control over the infrastructure, technology and data that power advanced information technology, cloud and AI systems. This trend reflects a fundamental shift in how Canada views digital capacity, recognizing it not as a convenience but as an essential pillar of economic resilience and national security in a shifting geopolitical landscape.

WHERE WE WERE IN 2025

The federal government's Sovereign AI Compute Strategy, announced in late 2024, marked a turning point for Canada. Backed by a $2 billion investment over five years, the strategy aims to close Canada's high-performance computing gap and reduce reliance on foreign hyper-scalers. Its pillars include building public supercomputing facilities, funding private-sector projects through the AI Compute Challenge, and creating an access program for small and medium-sized enterprises. The 2025 federal budget also earmarked $334.3 million over five years for quantum technologies to anchor Canadian firms and advance defence-related applications, reinforcing the broader compute and digital sovereignty agenda. This commitment was reinforced with an additional $925.6 million for sovereign public AI infrastructure, signaling that compute power is now treated as a strategic national asset.

Industry developments mirrored this policy momentum. In September 2025, a Canadian telecommunications carrier launched Canada's first sovereign AI infrastructure and AI services hub in Rimouski, Québec. The facility runs on 99% renewable energy, uses advanced cooling systems to reduce water consumption, and offers end-to-end AI services such as training, fine-tuning, and deployment, entirely within Canadian jurisdiction. In December, another carrier partnered with a major university in Ontario for a sovereign supercomputing centre in Kingston, designed to protect Canadian data and intellectual property while accelerating research and commercialization. Following this development, academic institutions also stepped up: two computing centres at major universities in Ontario upgraded their clusters to support GPU-intensive AI workloads, reinforcing Canada's research backbone.

The push for sovereign AI infrastructure is driven by several factors. First, Canada's compute gap has become a strategic vulnerability. Without domestic capacity, Canadian researchers and businesses have to rely on foreign providers, exposing sensitive data and intellectual property to external jurisdictions with no guarantees that this access would be maintained in the medium to long-term. Second, global competition for AI leadership is intensifying, and nations with sovereign infrastructure are expected to have a clear advantage over those that do not as they will have the ability to steer priorities and leverage strengths. Finally, public trust depends on demonstrable control while Canadians expect that critical AI systems operate within Canadian laws and oversight.

Policy experts have consistently stressed that digital sovereignty is not just about location. Reports from The Dais (a Toronto-based public policy think tank) and Information and Communications Technology Council advocate for the need of a more comprehensive approach by covering hardware, software, supply chains, and governance, alongside sustainability and regional equity. These proposals advance AI infrastructure as a public utility, analogous to energy grids or transportation networks, where national control is paramount.

INDUSTRY RESPONSE AND GLOBAL ENGAGEMENT

In December 2025, a global computing and cloud service provider announced a $19 billion investment to expand Canadian data centres and AI capacity, including in-country processing and a Threat Intelligence Hub in Ottawa. While this will help close Canada's compute gap, it raises questions about long-term control and exposure to foreign laws such as the US CLOUD Act. The provider has pledged legal protections and continuity, but enforceable safeguards will be essential. Other AI organizations have explored building large-scale compute in Canada that may bring additional capacity but will require careful agreements to maintain digital sovereignty.

These developments highlight that while Canada needs both scale and speed in growth of AI compute capacity, digital sovereignty remains an ongoing concern. Canadian-owned facilities represent an important step toward digital sovereignty, but true sovereignty requires Canadian control over technology, governance, and legal frameworks, not just their physical location. Organizations will need to design architectures that prioritize portability and continuity, ensuring critical workloads remain under Canadian control and jurisdiction even if vendor relationships change.

FROM POLICY TO PRACTICE

The defining trend for 2026 will be execution. Public investments must translate into operational systems that researchers and businesses can access. Private projects need to deliver on time and at scale. The federal government's AI Compute Access Fund will play a crucial role in democratizing access, but success will depend on clear timelines, inter-operability, and cost structures that support widespread and uniform adoption. Continued focus will centre around expanding Canadian-controlled compute capacity, securing sovereign data pathways, and fostering innovation ecosystems that align with national priorities. In parallel, the federal government is moving to embed AI across departments and pursue a sovereign Canadian cloud approach, keeping sensitive workloads under Canadian control and jurisdiction. These efforts represent a direct flow-through from 2025 commitments, ensuring that Canada's early investments translate into scaled infrastructure and actionable outcomes in 2026.

Growth will be qualified by measurable milestones, such as operational readiness of sovereign facilities, increased access for small and medium enterprises through the federal government's AI Compute Access Fund, and integration of sustainability benchmarks. Governance will be just as important as infrastructure. Sovereign AI systems must include robust frameworks for accountability, transparency, and risk management. As a part of accountability, contracts should guarantee rights over data and models and allow Canadian authorities to inspect systems when needed. Sustainability will also remain a priority. Upcoming projects and facilities should demonstrate that energy efficiency and renewable power can be integrated into sovereign infrastructure, aligning technological progress with environmental goals.

For Canadian organizations, the message from government is clear: digital sovereignty is becoming a strategic priority. Businesses that rely on AI should begin mapping their workloads against sovereignty considerations, such as where AI processing infrastructure is located, where the underlying data is stored, where models are trained, and under whose laws operations are governed. We recommend that organizations also review contracts for portability and continuity provisions, ensuring they can maintain control in the face of geopolitical or legal disruptions. Another important consideration for adopting organizations is that boards and risk committees should treat digital sovereignty as a core element of their digital strategy, not a mere compliance checkbox.

LOOKING AHEAD

Ultimately, digital sovereignty is about agency. It enables Canada to innovate and partner globally on its own terms, protect critical assets, and ensure that the benefits of AI accrue to Canadian society. Public trust will be shaped by the success of Canada's sovereign AI strategy. In 2025, the groundwork was laid through policy and investment in infrastructure projects. In 2026, success will hinge on operationalizing that vision by turning commitments into operational capacity. Canadians expect these investments to deliver tangible benefits including national resiliency, control over strategic priorities, environmental responsibility, and transparency. If projects meet these goals, confidence will grow. If they do not, digital sovereignty risks being perceived as symbolic rather than substantive. Organizations should proactively align their strategies with sovereignty requirements to mitigate risk and maintain competitiveness.

Contacts

Fasken's Technology group is a recognized leader and one of the largest and longest-tenured technology law teams in Canada. Our national team has built a legacy of resolving our clients' most challenging IT issues. We have extensive experience acting for technology providers and users in connection with the development, protection, and commercialization of technology products and services, and assisting buyers and sellers with the acquisition and disposition of technology businesses.

We advise on everything from complex commercial IT transactions, including large systems implementations, outsourcing arrangements, and XaaS arrangements, to internet business models, e-commerce, new technologies (such as quantum computing, artificial intelligence, and blockchain), technology acquisitions/divestitures, and data protection.

Our team is here to help you achieve your business goals. For more information or to discuss a particular matter, please contact us.

Andrew S. Nunes
Partner | Toronto
+1 416 865 4510
anunes@fasken.com

Andrew C. Alleyne
Partner | Toronto
+1 416 868 3338
aalleyne@fasken.com

John Beardwood
Partner | Toronto
+1 416 868 3490
jbeardwood@fasken.com

Daniel Fabiano
Partner | Toronto
+1 416 868 3364
dfabiano@fasken.com

Gabriel M.A. Stern
Partner | Toronto
+1 416 865 5494
gstern@fasken.com

Christopher Ferguson
Partner | Toronto
+1 416 865 4425
cferguson@fasken.com

Ariel Laver
Partner | Vancouver
+1 604 631 3201
alaver@fasken.com

Karam Bayrakal
Partner | Vancouver
+1 604 631 4850
kbayrakal@fasken.com

Jocelyn Auger
Partner | Montréal
+1 514 397 7694
jauger@fasken.com

Paul Burbank
Partner | Toronto
+1 416 865 4427
pburbank@fasken.com

Shan L. M. Arora
Associate | Toronto
+1 416 865 5412
sarora@fasken.com

Summer Lewis
Associate | Toronto
+1 416 865 5490
slewis@fasken.com

Keihgan Blackmore
Associate | Toronto
+1 416 868 7870
kblackmore@fasken.com

Camille Malone
Associate | Vancouver
+1 604 631 3528
cmalone@fasken.com

Nareg Froundjian
Associate | Montréal
+1 514 397 7420
nfroundjian@fasken.com

Alexander J. Shapiro
Associate | Montréal
+1 514 657 2423
ashapiro@fasken.com

Anthony Foreshew
Articling Student | Toronto
+1 416 865 4464
aforeshew@fasken.com

Pahul Sond
Articling Student | Toronto
+1 416 865 4563
psond@fasken.com

FASKEN

Own tomorrow

ABOUT THE FIRM

As a premier law firm with over 900 lawyers worldwide, Fasken is where excellence meets expertise. We are dedicated to shaping the future our clients want, precisely when it matters most. For more information, visit fasken.com.

FASKEN

Own tomorrow

Fasken Martineau DuMoulin LLP

fasken.com