Data sovereignty and the CLOUD Act: What Canadian organizations should know

April 13, 2026

Data sovereignty has re-emerged as a central concern for Canadian organizations navigating an increasingly complex geopolitical and regulatory environment. At present, the underlying concern involves the power of U.S. government authorities, through the 2018 U.S. *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), to access the personal information of Canadians. At its core, the issue of data sovereignty raises a practical and pressing question: to what extent can foreign governments access personal information about Canadians when that data is processed using global infrastructure?

While often framed as a question of where data is stored, data sovereignty is better understood as a question of control, which is shaped by legal jurisdiction, corporate structure, and service provider relationships. As reliance on cloud computing and AI services grows, and as tensions between Canada and the United States sharpen policy debates around cross-border data flows, organizations are being forced to reassess long-standing assumptions about data residency, risk, and compliance.

This BLG Insight examines the legal and practical dimensions of data sovereignty, including the impact of U.S. lawful access laws, and offers guidance on how Canadian organizations can assess and manage these risks.

Key takeaways

As of 2026, decision-makers across Canada should remember what follows as they address data sovereignty in a changing legal and geopolitical landscape:

- **Data sovereignty is about control, not just location**. Storing data in Canada does not, by itself, prevent access under foreign laws; who controls the data matters more than where it is located.
- **U.S. law remains a central risk factor**. Under the CLOUD Act, U.S. authorities may compel U.S.-based companies — or foreign subsidiaries under U.S. control — to produce data, even if that data is stored in Canada and relates to non U.S. persons.
- **Corporate structure and operational control are critical**. A Canadian entity that is wholly owned and managed in Canada will generally fall outside the scope

of the CLOUD Act, but Canadian subsidiaries operating under meaningful U.S. parent control may still be subject to U.S. lawful access obligations.
- **A risk-based approach is required, focusing on legal exposure, data sensitivity, and operational realities**. Organizations should assess exposure to foreign laws together, rather than applying blanket localization rules.
- **PIAs are increasingly expected**. In Québec in particular, transferring personal information outside the province triggers a legal obligation to conduct a PIA that evaluates, among others, the applicable foreign legal framework.
- **Transparency is mandatory**. Organizations must clearly inform individuals when personal information may be processed outside Canada and could be accessed by foreign courts or authorities.
- **Data minimization and retention limits reduce exposure risk**. Collecting only necessary data, favouring encrypted, de identified or anonymized datasets, and securely destroying data once no longer required significantly limits exposure to foreign access.

Legal considerations relevant to data sovereignty

The term “data sovereignty” means ensuring that data collected, stored, or otherwise processed in Canada remains primarily subject to Canadian law. For organizations considering data sovereignty, the main question is not simply where data is stored (often referred to as “data localization”), but how the jurisdiction, corporate structure, and operational control collectively influence the lawful access risks posed by foreign governments.

The applicability of the CLOUD Act is a critical component of this analysis. The CLOUD Act permits U.S. authorities to compel the production of data that is within the “possession, custody or control” of a covered entity. A covered entity includes U.S. based companies and foreign companies subject to U.S. jurisdiction. A covered entity may also be a foreign subsidiary of a U.S. parent company, where the parent exercises substantial control over the subsidiary’s operations and retains sufficient possession, custody, or control over the data. In a nutshell, a U.S. company, or a foreign subsidiary operating under U.S. control, may be compelled to produce data even if that data is stored in Canada.

This means that the jurisdiction in which a company is incorporated may influence data sovereignty, but only in light of the specific factual circumstances involved. For instance, an entity incorporated in Canada that is wholly owned and managed in Canada will generally fall outside the scope of the CLOUD Act. By contrast, if a Canadian subsidiary operates under the direct control of a U.S. parent company, such as via integrated systems or shared management, U.S. lawful access requirements may still apply, regardless of the physical location of the data.

Canadian privacy regulators have consistently cautioned against relying solely on data localization to address data sovereignty risks. Instead, they emphasize the need to implement reasonable security safeguards based on context and to adopt a risk-based approach, weighing exposure to foreign laws like U.S. surveillance alongside cybersecurity threats and data sensitivity.

How to manage your data sovereignty risks

In light of the above considerations, Canadian organizations should adopt a proactive and risk-based approach to managing data sovereignty, which might include some of the following measures:

Risks assessment

Privacy regulators recommend assessing the risks that could jeopardize the integrity, security, and confidentiality of users' personal information processed by service providers operating outside of Canada to limit personal information risk exposure to foreign government access. A privacy impact assessment (PIA) is a critical tool to determine where data is processed, stored, and who has access to it. As part of this exercise, organizations should map data flows and identify service providers that may be subject to foreign legal regimes.

Québec has led the way in Canada and requires organizations entrusting a person or body outside Québec with the task of collecting, using, communicating, or keeping such information on their behalf to conduct a PIA. The PIA must especially consider the legal framework applicable in the jurisdiction in which the information would be transferred, including the personal information protection principles applicable in that jurisdiction, in light of generally recognized principles regarding the protection of personal information inspired by the OECD Privacy Guidelines, the U.S. Federal Trade Commission's Fair Information Practice Principles (FIPPs), Canada's federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and the European Union's *General Data Protection Regulation* (GDPR); see Cross-border transfers of personal information outside Québec: Requirements for businesses.

Transparency

Be transparent and inform users of risks about personal information handling practices, especially that their personal information may be processed in other jurisdictions and that it may be accessed by the courts, law enforcement, and national security authorities of other countries. This is a requirement under Canadian personal information protection laws that has always been emphasised by privacy regulators. In practice, this might involve updating privacy policies and vendor disclosures to clearly address cross-border processing and lawful access risks.

Data minimization and retention

Limitations to data collection and retention can also serve as effective data sovereignty safeguards to mitigate risk exposure. Data minimization is a fundamental principle of Canadian personal information protection laws that can significantly reduce privacy and cyber risks (see Less is more – Data minimization and privacy/cyber risk management).

When collecting and retaining only personal information that is strictly necessary, access by foreign governments would be limited solely to data stored. Data minimization is not only a question of volume, but also of the nature of the data. As a result, organizations should consider using encrypted, aggregated, deidentified, or anonymized datasets whenever possible to reduce identification risks. In addition, information should only be retained for the legally and effectively required periods of

time, and then promptly, securely destroyed to limit the timeframe during which personal information may be accessed.

Conclusion

In an era of cross-border cloud infrastructure and geopolitical uncertainty, data sovereignty for Canadian organizations is ultimately about control, not just physical location. A practical response is therefore risk-based: understand and document data flows, assess exposure through PIAs, require clear transparency to individuals, and reduce the amount and identifiability of data through minimization, retention limits, and strong safeguards. Taken together, these measures can help organizations manage sovereignty risk while continuing to benefit from global technology services.

By

Claire Feltrin, Candice Hévin, Andrea Imola

Expertise

Cybersecurity, Privacy & Data Protection, Privacy Impact Assessments (PIAs), Compliance with Privacy & Data Protection, Information Technology, United States

---