GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

RECOMMENDATIONS ON BILL C-36 CROSS-BORDER DATA PROVISIONS

SUBMITTED TO STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY, CANADIAN HOUSE OF COMMONS

August 2026

The Global Data Alliance (GDA) welcomes the opportunity to provide feedback on Bill C-36 and, specifically, the bill's treatment of cross-border data transfers. GDA supports the bill's objective of ensuring that personal information remains protected when it is transferred outside Canada. We respectfully recommend, however, that Bill C-36 preserve Canada's longstanding accountability-based approach to international transfers and avoid imposing an across-the-board assessment requirement that is not calibrated to risk.[1]

The GDA is a cross-industry coalition of companies headquartered across multiple regions of the world that are committed to high standards of data privacy, security, and responsible data use. GDA members share a long-standing commitment to supporting economic development, building trust in the digital economy, and protecting personal and non-personal data across jurisdictions, technologies, and business models. Alliance member companies rely on the ability to transfer data responsibly across borders to innovate, create jobs, and make industries more competitive in their home markets and abroad. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors.

Our comments focus exclusively on Section 57, which would require an organization, before disclosing or transferring any personal information outside Canada, to conduct an impact assessment and implement measures to mitigate the identified risks. GDA recommends that the Committee remove this requirement and retain the existing accountability framework that already exists in Canadian law. If the Committee retains Section 57, the provision should be narrowed, made explicitly risk-based, and implemented in a way that recognizes equivalent Canadian and international safeguards.[2]

I. Cross-Border Data Transfers Support Every Sector of Canada's Economy.

Cross-border data transfers are critical to the modern Canadian economy. Canadian organizations routinely rely on global cloud infrastructure, cybersecurity providers, fraud prevention services, customer support operations, research partners, payment systems, and other specialized services located in multiple jurisdictions. These transfers support productivity, innovation, safety, cybersecurity resilience, environmental sustainability, and access to global markets.[3]

---

[1] For more information about the Global Data Alliance, see https://www.globaldataalliance.org.

[2] Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, 45th Parliament, 1st Session, Section 57, https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading.

[3] See Global Data Alliance, Cross-Border Data Policy Index, https://globaldataalliance.org/resource/cross-border-data-policy-index/

All Canadian businesses benefit from cross-border access to technology and data, as well as the ability to move information seamlessly and securely across digital networks. Manufacturers, including automotive and aerospace companies, use operational and supply-chain data to coordinate production across North America. Agriculture, energy, and natural-resource companies use remote sensing, predictive maintenance, and global analytics to improve safety and efficiency. Financial institutions and insurers use cross-border threat intelligence and fraud monitoring to protect customers. Healthcare and life-sciences organizations collaborate across borders on research, safety monitoring, and medical innovation. Canadian small and medium-sized enterprises rely on cloud-based payments, logistics, customer support, and security tools to reach customers beyond Canada without building costly infrastructure in every market.

Cross-border processing can also strengthen privacy and security. Globally distributed infrastructure can provide redundancy, rapid threat detection, around-the-clock security monitoring, and access to specialized expertise that may not be available in every country. The physical location of data is therefore not, by itself, a reliable measure of whether the data is protected. The relevant questions are whether the organization remains accountable, whether the transfer is supported by appropriate contractual, technical, and organizational safeguards, and whether those safeguards are proportionate to the sensitivity and risk of the processing.

Canada's international commitments reflect the same basic approach. CUSMA Article 19.11 and CPTPP Article 14.11 require the parties to allow cross-border transfers of information, including personal information, for covered business activity, while preserving authority to pursue legitimate public policy objectives through measures that are not arbitrary, discriminatory, disguised restrictions on trade, or more restrictive than necessary. Bill C-36 should reinforce that balance by protecting personal information through accountable and proportionate safeguards rather than treating every international transfer as presenting the same level of risk.[4]

II. Bill C-36 Should Preserve PIPEDA's Accountability-Based Approach.

GDA strongly supports PIPEDA's current approach to international data transfers – an approach that rests on organizational accountability. For more than two decades, Canada's federal privacy framework has recognized that organizations may transfer personal information across borders for processing, provided that the transferring organization remains accountable and uses contractual or other means to provide an appropriate level of protection. The Office of the Privacy Commissioner of Canada has described this as an organization-to-organization approach and has confirmed that PIPEDA does not prohibit international transfers for processing.[5]

This framework protects Canadians because accountability follows the data. It places responsibility on the organization that knows the purpose of the processing, selected the service provider, and maintains the relationship with the individual. It also gives organizations flexibility to use safeguards suited to the transfer, including contract terms, access controls, encryption, audit rights, incident-response obligations, and limits on onward transfers.

---

[4] See Canada-United States-Mexico Agreement, Article 19.11, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=eng; Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Article 14.11, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

[5] Office of the Privacy Commissioner of Canada, Guidelines for processing personal data across borders, https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/.

Regrettably, Section 57 would replace that adaptable, durable, and longstanding approach with a rigid, mandatory assessment triggered by geography rather than risk. The requirement applies before any disclosure or transfer outside Canada, regardless of the sensitivity of the personal information, the purpose of the transfer, the safeguards already in place, or whether the transfer is routine and recurring. Because the prescribed assessment requirements are not yet known, organizations would also face substantial uncertainty about whether one assessment may cover a recurring transfer, a class of transfers, or an enterprise-wide processing arrangement.

Transfer assessments can be highly complex and resource-intensive. An obligation that applies indiscriminately to all international transfers would fall particularly heavily on smaller Canadian organizations, which often depend most on affordable global cloud, security, and business services. It could also delay the deployment of security updates, fraud-prevention tools, and other services that protect individuals. GDA therefore recommends removing Section 57's mandatory assessment requirement and retaining PIPEDA's accountability principle as the foundation for international transfers.

III. Any Retained Assessment Requirement Should Be Risk-Based, Reusable, and Interoperable.

If the Committee retains Section 57, the bill or implementing regulations should narrow the obligation to transfers that are reasonably likely to create a high risk to individuals. Routine transfers of non-sensitive personal information, transfers involving data protected through effective encryption or pseudonymization, and processing conducted under an approved or widely recognized transfer mechanism should not require the same analysis as a transfer of highly sensitive data without established safeguards.

The law should also permit one assessment to cover a recurring transfer, a defined category of transfers, or a continuing service arrangement. An assessment should need to be updated only when there is a material change in the data, purpose, destination, recipient, legal environment, or safeguards. Requiring a new assessment for each transaction or each movement of data within distributed infrastructure would produce paperwork without improving privacy protection.
Bill C-36 should also avoid duplicative Canadian assessments. For example, Section 17 of Quebec's Act respecting the protection of personal information in the private sector already requires a privacy impact assessment before personal information is communicated outside Quebec. Where an organization has completed a substantively equivalent assessment under Quebec law or another applicable Canadian requirement, Section 57 should deem that assessment sufficient for the same transfer unless a material change requires an update.[6]

The required assessment should also be clearly labeled a transfer impact assessment. Section 18(4) uses the term privacy impact assessment for a separate assessment connected to legitimate-interest processing. Using the same term for distinct obligations creates avoidable confusion about their scope, content, and recordkeeping.

Finally, Section 57 should allow organizations to rely on safeguards and assessments already established under trusted international mechanisms. Compliance with mechanisms such as the Global Cross-Border Privacy Rules System, the EU Standard Contractual Clauses, the UK International Data Transfer Agreement, binding corporate rules, and recognized privacy or security certifications should satisfy, or at minimum create a presumption of compliance with, the assessment and mitigation obligations. This approach would encourage strong, enforceable safeguards while reducing duplicative

[6] Act respecting the protection of personal information in the private sector, CQLR c P-39.1, Section 17, https://legisquebec.gouv.qc.ca/en/showdoc/cs/p-39.1.

work and supporting interoperability between Canada's framework and those of its major trading partners.[7]

Recommendations

- **Retain PIPEDA's accountability-based approach** to cross-border transfers, under which an organization remains responsible for personal information regardless of where it is processed.
- **Remove Section 57's mandatory assessment requirement** for disclosures and transfers outside Canada.
- **If Section 57 is retained, limit it to high-risk transfers** and permit one assessment to cover recurring or related transfers, with updates required only after a material change.
- **Avoid duplicative assessments** by recognizing substantively equivalent assessments completed under Quebec law, other Canadian requirements, or trusted international frameworks.
- **Recognize leading transfer mechanisms** including the Global CBPR System, EU SCCs, UK IDTA, binding corporate rules, and recognized certifications, as satisfying or presumptively satisfying any retained assessment and mitigation requirement.

* * *

The GDA appreciates the opportunity to provide these comments. A modernized Canadian privacy law should protect personal information wherever it is processed while preserving the trusted data flows on which Canadian individuals, businesses, researchers, and public-interest institutions depend. We would welcome the opportunity to discuss these recommendations further.

[7] See Global CBPR Forum, https://www.globalcbpr.org/; European Commission, Standard Contractual Clauses, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; UK Information Commissioner's Office, International transfers, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/.