Last Updated: September 2025

AUTODESK

FAQs re: British Columbia & Alberta Privacy Regulations (Canada)

What are the privacy laws in British Columbia and Alberta?

The provinces of British Columbia and Alberta each have specific privacy legislation that regulates the management of personal information by private sector organizations:

- **British Columbia Personal Information Protection Act (BC PIPA)[1]:** This statute applies to private-sector organizations operating within British Columbia. It sets out rules governing the collection, use, and disclosure of personal information in the course of commercial activities.
- **Alberta Personal Information Protection Act (Alberta PIPA)[2]:** Similarly, this act governs how private-sector organizations in Alberta handle personal information. Its provisions are designed to ensure organizations manage such data responsibly and transparently.

In addition to PIPA, both provinces have legislation covering public bodies:

- **Freedom of Information and Protection of Privacy Act (FOIPPA – British Columbia):** Applicable to provincial ministries, agencies, crown corporations, and local governments in British Columbia, this legislation provides individuals with the right to access information held by public bodies and establishes requirements to protect personal information.
- **Freedom of Information and Protection of Privacy Act (FOIP – Alberta):** This act is in force for public bodies in Alberta, including government departments, agencies, and municipalities. It similarly grants access rights and mandates safeguards for the personal data managed by these entities.

Together, these laws form a comprehensive framework for privacy protection in both public and private sectors within British Columbia and Alberta.

Do these laws apply to organizations outside of Canada?

Yes, these provisions apply to any private sector organization that collects, uses, or discloses individuals' personal information within these regions.

---

[1] British Columbia Personal Information Protection Act (BC PIPA). Available at: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01 (Accessed: 25 July 2025).

[2] Alberta Personal Information Protection Act (Alberta PIPA). Available at: https://www.alberta.ca/personal-information-protection-act (Accessed: 25 July 2025).

What is “personal information” under BC and Alberta PIPAs?

"Personal information" refers to data pertaining to an identifiable individual. This encompasses names, email addresses, IP addresses, contact details, and any other information that can be associated with a person, either directly or indirectly.

Is consent needed to collect personal information in these provinces?

Consent is the foundational principle underpinning both British Columbia and Alberta's Personal Information Protection Acts (PIPA). Implied consent may be deemed appropriate in circumstances that present minimal risk. However, express consent is required when dealing with sensitive information, when the intended use of the data is not immediately evident, or when the information is to be disclosed to third parties.

Are companies required to notify individuals of their data practices?

Yes. The following information must be clearly communicated: the purpose for which personal information is being collected, the intended uses of such information, the parties with whom the information may be shared, and contact details for any privacy-related inquiries.

Is there a requirement to have a local representative or physical presence in BC or Alberta?

No, but if a covered entity targets residents of these provinces, the covered entity is subject to the applicable PIPA and may need to designate a privacy officer.

Is there a requirement to notify individuals or regulators in the event of a data breach?

In Alberta, breach reporting is mandatory if there is a real risk of significant harm. In contrast, British Columbia does not require breach reporting by law; however, it is strongly encouraged.

Are contracts with third-party service providers required?

Yes. Covered entities are required to ensure that their third-party service providers offer a comparable level of protection for personal information. This obligation should be established through written agreements that clearly outline privacy and security expectations. Additionally, organizations are advised to monitor vendor compliance with these requirements when applicable.

Can we transfer personal data outside of Canada?

Yes; however, covered entities are required to disclose international data transfers to users, specify the jurisdictions involved, and implement appropriate safeguards such as contractual agreements and risk assessments.

Do individuals have access and correction rights?

Individuals are entitled to exercise their rights to access and request corrections to their personal information held by covered entities. Organizations are required to respond to

such requests within 45 days, ensuring that any inaccuracies or incomplete data are rectified promptly in accordance with privacy regulations.

What are the penalties for non-compliance?

In Alberta, organizations found to be in violation of the province's privacy legislation may face fines of up to $100,000 CAD for each offence. In British Columbia, while the enforcement measures are generally less stringent, non-compliant entities are still subject to formal orders and significant reputational risks, which can have considerable consequences for their operations and public standing.

Do covered entities need to conduct Privacy Impact Assessments (PIAs)?

Although Privacy Impact Assessments (PIAs) are not mandated by PIPA, they are widely regarded as a best practice. Organizations are advised to conduct a PIA when introducing new products or features, handling sensitive personal information, deploying artificial intelligence technologies, or transferring personal data internationally. Performing these assessments enables organizations to identify, assess, and mitigate potential privacy risks, thereby supporting regulatory compliance and strengthening the trust of individuals whose data may be impacted.

How Does Autodesk Comply with these Laws?

Autodesk has incorporated its disclosure and individual rights obligations into its global privacy program. For more information, including information on how individuals can exercise their rights under State Privacy Laws at Autodesk, please see Autodesk's Privacy Statement and Autodesk's Trust Center Privacy page.