**WHAT IS CANADA'S PIPEDA?**

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian federal law enacted in April 2000 that governs the way organizations collect, use, and disclose the personal information of Canadians.

**DOES PIPEDA APPLY TO ORGANIZATIONS OUTSIDE OF CANADA?**

PIPEDA applies to organizations outside of Canada that have a "real and substantial" connection to the country. Guidance issued by the Office of the Privacy Commissioner (OPC) suggest organizations consider factors such as the location of the end user, where the activity takes place, and the jurisdiction where promotional efforts are primarily targeted to determine whether they fall within PIPEDA's extra-territorial jurisdiction.

The law also applies to international and interprovincial transfers of personal information. PIPEDA provides protections similar to the General Data Protection Regulation (GDPR) and allows for transfers of personal data between Canada and the European Union.

**HOW DOES PIPEDA DEFINE PERSONAL INFORMATION?**

Personal information means information about an identifiable individual. Generally, information is considered identifiable when there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

PIPEDA does not define sensitive personal information, but guidelines state that medical records, financial records, and the like are highly sensitive and require additional protection.

**WHAT OBLIGATIONS DO ORGANIZATIONS HAVE UNDER PIPEDA?**

Organizations must comply with 10 enumerated principles (e.g., accountability, limiting the collection and use of information) and must protect personal information with safeguards proportionate to the sensitivity of the information. Safeguards should include physical, organizational, and technological measures.

Generally, organizations may only process personal information with an individual's knowledge and meaningful consent. Consent may be implied, but express consent is required for collections, uses or disclosures which generally: (i) involve sensitive information; (ii) are outside the reasonable expectations of the individual; and / or (iii) create a meaningful residual risk of significant harm.

When transferring personal information to third parties, organizations must use contractual privacy protection clauses or other measures to require the third party to provide a comparable level of protection to the information being processed. The organization remains responsible for the personal information.

Organizations must also name an individual responsible for privacy practices, and provide notices that include the following:

- the name and contact information of:
    - the person responsible for privacy practices and policies; and
    - the person to whom access requests should be sent;

- a description of what personal information is disclosed to other organizations, including subsidiaries and third parties;
- a list of the PIPEDA rights for consumers;
- how an individual can exercise those rights and submit complaints;
- information the individual must provide to verify their identity to exercise their rights.

**WHAT RIGHTS DO INDIVIDUALS HOLD UNDER PIPEDA?**

- to access the personal information that an organization holds about them;
- to correct or complete that personal information;
- to withdraw consent to the processing of their personal information; and
- to lodge a complaint about the processing of their personal information with the authorities.

**DOES PIPEDA CREATE SPECIAL RULES FOR MINORS?**

Not specifically. The OPC views a minor's personal information as being particularly sensitive and released guidance regarding the collection, use, and disclosure of a minor's personal information. Among other things, the guidance suggests limiting (or avoiding altogether) the collection of minors' personal information, implementing defaults appropriate to the age of users, considering the user experience, and preventing the unauthorized use of children's information.

**HOW DOES AUTODESK COMPLY WITH PIPEDA?**

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.

**DOES PIPEDA PROVIDE A PRIVATE RIGHT OF ACTION FOR INDIVIDUALS?**

PIPEDA does not establish a general private right of action.[1] Instead, PIPEDA permits individuals that file complaints regarding potential violations of PIPEDA to apply to the Federal Court for a hearing for damages, including damages for "humiliation," about matters referenced in the Complaint or the OPC's report. The Federal Court may also order the breaching organization to correct its practices. Such applications may only be brought after the complainant has received a report of findings or a notice of discontinuance of the investigation of the claim from the OPC. Further, the scope of this right is limited to violations of certain provisions under PIPEDA, such as provisions relating to contracting requirements with third parties and transparency requirements.

The OPC may initiate an audit when it has reasonable grounds to believe an organization is not complying with the law. Organizations that willfully violate PIPEDA or obstruct the Commissioner's investigation/audit may be guilty of an offense punishable on summary conviction and liable for a fine for up to $10,000 CAD or an indictable offense and liable for a fine for up to $100,000 CAD.

[1] Canada's draft Consumer Privacy Protection Act (Bill C-27), prepared with the aim of replacing PIPEDA, introduces a new private right of action for individuals. Local counsel expects Bill C-27 will be adopted some time in 2024.

**WHAT MUST HAPPEN IN THE EVENT OF A BREACH?**

PIPEDA requires an organization to notify affected individuals of any breach involving personal data under its control as soon as feasible if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Organizations must also report the breach to OPC and keep records of all breaches for two years.

**ARE THERE ANY OTHER FEDERAL LAWS GOVERNING ELECTRONIC COMMUNICATION IN CANADA?**

Organizations must also comply with Canada's Anti-Spam law – CASL. CASL prohibits the sending of commercial electronic message without 1) the recipient's consent or 2) the sender's contact information and an unsubscribe mechanism.

Section 8 of CASL also requires organizations that, in the course of a commercial activity, install or cause to be installed a computer program, including cookies, on another person's computer system to obtain express consent from the owner or authorized user of the computer system. This being said, the installation of cookies on a user's device is permitted without requesting express consent as long as it is reasonable to believe that the device user consents to the program's installation based on the user's actions. According to guidance issued by the Canadian Radio-television and Telecommunications Commission (CRTC) this means that at the very least, an organization must avoid installing cookies if a user disables them in their browser, though there may be other circumstances where express consent is required.