

Fortra, PIPEDA, and You

The Personal Information Protection and Electronic Documents Act (PIPEDA) became law in Canada in April 2000 and has been reviewed and updated every five years since. The act was also intended to promote consumer trust in electronic commerce and also to reassure the European Union that Canadian privacy laws sufficiently protected the personal information of European citizens.

PIPEDA applies to Canadian organizations that are federally regulated such as the telecommunications and broadcasting industry, and also applies to private sector organizations operating in provinces that have not enacted similar privacy laws of their own. To date, only the provinces of British Columbia, Alberta, and Quebec have privacy laws that have been deemed to be “substantially similar” to PIPEDA. However, even if a provincial regulation exempts an organization from PIPEDA for intra-provincial business, PIPEDA will still apply during cases in which commercial activity crosses provincial borders.

Businesses must follow the 10 fair information principles to protect personal information, which are set out in Schedule 1 of PIPEDA. These principles form a mechanism and a roadmap for organizations doing business in Canada to build and maintain consumer trust in the digital economy.

How Fortra Helps Organizations Follow the Privacy Principles of PIPEDA

• **Accountability**

- The principle of Accountability states that organizations must designate someone who, among other duties, must develop procedures to protect personal information and also develop materials to train staff and communicate this information internally and externally. The person chosen to take on these responsibilities will most definitely be a subject matter expert, but it is less common for them to be experts in personal data identification and protection.
- Choosing Fortra Data Classification Suite (DCS) grants access to proven methodology built on experience and best practices to take the guesswork out of privacy protection. The blueprint for success that comes with every Fortra deployment maps security requirements with positive outcomes for your business while providing real-time continuous training to the entire organization.

HIGHLIGHTS

- In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the collection, use, and disclosure of personal information by private sector organizations
- Makes organizations accountable for the protection of personal information under their control
- Applies to any organization engaging in commercial, for-profit activities
- Non-compliant organizations face fines of up to \$100,000

• Limiting Use, Disclosure, and Retention

- The principle of Limiting Use, Disclosure, and Retention states that an organization must limit the ways it uses, discloses and retains personal information. Organizations must not use or disclose personal information for purposes other than those which it has identified purposes for and received consent for. Furthermore, organizations must not retain personal information any longer than is necessary to fulfill its purposes.
- The persistent metadata applied when files are classified with Fortra that can uniquely identify any categories to which the file belongs and can be customized to include the purposes for holding said files. Retention terms and required dates of deletion can also be included with the file to take the guesswork out of compliance.

• Safeguards

- Organizations must protect personal information with security safeguards that are appropriate for the sensitivity of personal information held. Personal information should be protected against loss or theft, unauthorized access, disclosure, copying, use or modification.
- Fortra metadata can be leveraged by other security solutions, such as data loss prevention (DLP), enterprise rights management (ERM), cloud access security brokers (CASB), and next generation firewalls to enforce the data protection policies required to keep data safe.

• Individual Access

- This principle states that individuals have a right to access the personal information that an organization holds about them. They also have the right to challenge the accuracy and completeness of the information, and have that information amended or deleted as appropriate.
- Fortra's DCS for Data at Rest file analytics software takes the fear, uncertainty, and doubt out of Data Subject Access Requests by crawling fileshares – on premise and in the cloud – to discover where your personal data exists, who has access to it and more.

• Challenging Compliance

- The principle of Challenging Compliance means organizations must have procedures in place to receive and respond to complaints and inquiries from customers' challenges to their compliance to any of the privacy principles of PIPEDA.
- While organizations can adhere to the strict letter of the regulation by merely providing a mechanism for complaints, companies that deploy Fortra earn the piece of mind that comes with knowing that their entire workforce is involved and aware of the privacy principles included in not only PIPEDA, but also the principles of sound data governance.



Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.