Avaya Canadian Privacy Laws Compliance Guide

At Avaya security and privacy are of primary importance. Avaya is committed to building on its experience through leading edge technology solutions that enhance privacy, as well as cloud solutions that aim to deliver both security and privacy.

This includes complying with local and regional privacy and security regulations and giving Avaya's customers the tools they need to be compliant with Canadian data protection regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA), British Columbia's Personal Information Protection Act (BC PIPA), Alberta's Personal Information Protection Act (AB PIPA) and Quebec's Act Respecting the Protection of Personal Information in the Private Sector (the Quebec Act).

Avaya's commitment to privacy and security extends to implementing organization-wide policies and practices and physical and technical security measures aimed at promoting security and privacy of customer data, including personal information. As part of Avaya's Trust Center, Avaya publishes additional information about our security practices, including information about Avaya's certifications and accreditations. While Avaya prohibits the use of its services to breach privacy laws, Avaya cannot prevent all abuses of its services. Customers are responsible for their compliance with privacy laws and for ensuring their staff comply with privacy laws.

This document describes Avaya's privacy and security practices and how Avaya can help Canadian customers comply with Canadian private sector privacy laws.

1. What are PIPEDA, BC PIPA, AB PIPA and the Quebec Act?

PIPEDA is a Canadian federal privacy law and BC PIPA, AB PIPA and the Quebec Act are provincial counterparts to PIPEDA. Each of these laws regulates the collection, use and disclosure of individuals' personal information by private sector organizations. Personal information under these laws is any information about an identifiable individual.

2. How Avaya Helps Customers Meet Their Obligations

Avaya has implemented privacy practices and technical and physical security measures to protect customer data, including personal information.

(a) Avaya's Privacy Practices to Help Customers Meet Their Obligations

Avaya's privacy practices include:

- ensuring that Avaya complies with applicable laws when it collects, uses and discloses personal information.
- assisting customers in complying with requirements to inform and explain to individuals how their personal information is collected, used or disclosed.
- enabling customers to respond to requests from individuals for access to or correction of personal information.

- only using and disclosing personal information on behalf of a customer in accordance with the instructions of the customer and informing customers of when it cannot comply with this practice.

- following instructions of customers to return, destroy or store personal information in a secure manner when the services are terminated.

- following instructions of customers to provide assistance in keeping personal information accurate and up-to-date.

- complying with data security breach notification requirements and notifying customers of any security breach of personal information without undue delay and as required under its contracts with customers. Avaya also assists customers in complying with data security breach notification obligations.

- committing to help customers meet their compliance audit requirements.

- storing personal information in jurisdictions outside of Canada only as permitted by PIPEDA, the Quebec Act, AB PIPA and BC PIPA. Upon request, Avaya can provide product-specific information regarding storage location.

(b) Avaya's Physical and Technical Measures to Help Customers Meet Their Obligations

Avaya's physical and technical measures to promote data privacy and security include:

- restricting physical access to customer data processing equipment, including by:
    - an electronic access control system,
    - 24/7 video recording of physical facilities,
    - intrusion detection or engaging on-premises security officers, and
    - restricting access to various zones at is premises based on roles and periodically revalidating access.
- restricting logical access to customer data and processing equipment, including through:
    - unique user IDs for access with formal authorization processes and unique complex passwords,
    - role-based access, least-privileged access and need-to-know only access,
    - access logs,
    - multi-factor authentication of Avaya's VPN for remote access,
    - encrypted endpoints,
    - centrally monitored and updated anti-virus programs and regular anti-virus scans,

- secure deletion and/or disposal of data, and
- secure storage of backup media and testing backups.

- using secure communication channels and logging, including:
  - using VPN with a multi-factor authentication for remote access,
  - using firewalls with stateful inspection, default denial access rules, role-based and least-privileged access on a “need to know” basis, logging and alerting of access, an annual review, and
  - using encrypted email if this has been enabled by the customer, using TLS.

(c) Avaya’s Data Breach Incident Response Team and Privacy Law Advisors

Avaya also has a Data Breach Incident Response Team (DBIRT) that provides leadership in the event of a data breach. This is a cross-functional team established with the specific purpose of responding to actual and suspected data breaches. The DBIRT operates according to Avaya’s Data Breach Incident Response Plan, which provides a well-defined, organized, repeatable and documentable approach to efficiently and effectively respond to data breaches to minimize their impact on Avaya or third parties, including Avaya’s customers.

Avaya also receives advice from a leading Canadian law firm on privacy law compliance.

3. Who to Contact about Avaya’s Security and Privacy Practices

For any questions about Avaya’s security and privacy practices, please contact:

Avaya Global Privacy Office

Email: dataprivacy@avaya.com