RingCentral

Freedom of Information and Protection of Privacy Compliance Guide

July 2021

RingCentral and the Freedom of Information and Protection of Privacy in Canada

RingCentral takes all customers' data privacy and security seriously. This includes formal compliance with applicable local and regional laws and regulations. As a leading global communications and collaboration cloud service provider, RingCentral's platform services are designed to help our customers meet their compliance obligations under the Canadian freedom of information and protection of privacy regulations ("FOIPPA").

In this whitepaper, we provide information to help customers understand the FOIPPA regulations that govern the different provinces of Canada, including, for example, British Columbia and Ontario, and how they fit with RingCentral services. Customers that are subject to FOIPPA regulations are responsible for complying with its requirements. Since there is no officially recognized certification for FOIPPA regulations, such as SOC, PCI, or ISO, here we offer our customers information regarding the policies, processes, and controls established and operated by RingCentral.

Background	Access and privacy rights of individuals are protected by a number of privacy laws and regulations in Canada. In general, the collection, use and disclosure of personal information within the commercial sector is regulated by federal privacy legislation—the Personal Information Protection and Electronic Documents Act (PIPEDA). FOIPPA regulations in British Columbia, Ontario, and elsewhere in Canada generally govern access and privacy rights relating to the public sector. Specifically, FOIPPA regulations establish an individual's right to access personal information in the custody or control of public bodies in the respective province (e.g.,

	British Columbia, or Ontario) and sets out the terms under which the public body can collect, use and disclose such personal information. Under FOIPPA regulations, public bodies are required to protect personal information by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of such personal information. These regulations may also limit the transfer and access of data out of Canada in certain circumstances.
How RingCentral Helps Customers Meet Their Needs Under Applicable FOIPPA Regulations	We implement numerous measures to protect our customers' data, but our services are not designed to recognize or classify personal information that is subject to FOIPPA. RingCentral does not access customer content to determine whether it contains such personal information. Whether content (such as voicemails or recordings) includes such personal information or not, RingCentral applies the same processes and safeguards set forth in this whitepaper. Customers are responsible for using our services in compliance with the legal requirements that apply to them and they should consult their own legal advisors to understand the applicable privacy laws. The following information in this whitepaper explains how we support our customers in protecting personal information subject to FOIPPA.
Access & Correction Rights	FOIPPA regulations generally provide individuals with the right to access, correct, and in some circumstances, ask for the removal or modification of their data. RingCentral provides tools that allow customers to handle individual access requests; customers' account administrators can easily manage these in the Admin Portal for RingCentral's Services. For any further help with such requests, customers can also contact the RingCentral support team through a dedicated DSAR Portal. If an individual submits a request directly to RingCentral, RingCentral will direct the individual to contact the customer.
Security	FOIPPA regulations generally require organizations to apply technical controls to ensure the security of personal information in their custody or control. RingCentral's commitment to data security is demonstrated through the adoption of numerous security measures. These measures have been independently verified by outside parties. RingCentral regularly undergoes SOC 2, ISO 27001, ISO 27017, ISO 27018, and HITRUST audits. Current customers can access these audit reports directly through our Trust Portal. Our security measures include: • **Information Security Management**, including a written security program, security policy management, and risk management. • **Independent Security Assessments**, including SOC 2 Type II and IES/ISO 27001.

	• **Human Resource Security**, including background checks, training, data loss prevention, and subcontractors' due diligence. • **Physical Security**, including restricted access to secure areas, documented access authorization process, and security of its data centers. • **Logical Security**, including user identification and authentication, user authorization and access control. • **Telecommunication and Network Security**, including network management, network segmentation, and network vulnerability scanning. • **Operations Security**, including asset management, configuration management, malicious code protection, vulnerability and security patching, logging and monitoring. • **Data Classification and Handling**, including encryption and destruction of data. With respect to training, RingCentral will ensure that all employees, including contractors, complete annual training: (i) to demonstrate familiarity with RingCentral's security policies, and (ii) for security and privacy requirements, including CyberSecurity awareness, GDPR, and CCPA, and have the reasonable skill and experience suitable for employment and placement in a position of trust within RingCentral.
Openness	RingCentral is fully transparent about the ways it handles customer data. Information regarding RingCentral's practices relating to the management of personal information is listed in our Privacy Notice. The Privacy Notice also includes information on how to contact RingCentral's Privacy Office.
Storage of Personal Information	In some provinces, such as for example British Columbia, the applicable FOIPPA regulations may allow public bodies to store and provide access to personal information outside of Canada where individuals have provided the prescribed consent, or where the purpose for such storage and access is otherwise permitted by the law. For example, personal information may be disclosed outside Canada for temporary processing,[1] or if the personal information is metadata generated by an electronic system that describes an individual's interaction with the system and meets the other requirements of the law.[2] RingCentral provides customers with the information they need to determine whether its processing of personal data outside of Canada is permissible, or if individual consent is required.

[1] See British Columbia FOIPPA, Section 33.1(1)(p.1).
[2] See British Columbia FOIPPA, Section 33.1(1)(p.2).

RingCentral in Canada	As a leading provider of global enterprise cloud communications and collaboration solutions, RingCentral is constantly investing to expand its global offerings and localized features in Canada. For example, RingCentral offers bilingual apps in both English and French, and has recently launched a data center in Canada to support in-country failover and uptime of RingCentral's services. RingCentral continues to focus on businesses in Canada, and will continue to revisit opportunities to increase in-country data processing capabilities over time.
Limiting Use, Disclosure, and Retention	RingCentral will retain customer data only for the duration of the contract. Some data types will be automatically deleted even sooner than that. Customers are always in full control of their data. Ultimately, though, the customers are responsible for ensuring that they limit the use and disclosure of personal information only to the purposes for which it was collected. Additional information may be found at the RingCentral Support Portal.
Accuracy	When customers use the RingCentral services to collect or store personal information, RingCentral ensures that it is unchanged. RingCentral has put in place various security measures to guarantee the integrity of such information. For more details on these security measures, please see the "Security" topic above. Ultimately, the customers are proactively responsible for ensuring that the personal information collected and used is accurate.
Notice of Foreign Demands for Disclosure	From time to time RingCentral may receive data requests from law enforcement and government agencies around the world relating to a RingCentral customer account. In furtherance of RingCentral's commitment to maintaining the privacy and trust of our customers, RingCentral will reject or challenge requests that are, among other reasons, not accompanied by any valid legal process or valid legal basis. Further, RingCentral will notify its customers of any data request to enable them to respond to the request directly, unless RingCentral is precluded from doing so by law or court order. RingCentral reserves the right to respond or object to any request for data in any manner consistent with applicable law.

RingCentral

727750436 07/2021

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com