ComputerTalk Cloud Services Privacy Policy

March 2023

Version 1.40

Computer Talk Technology Inc.

150 Commerce Valley Drive West, Suite 800
Markham, Ontario, Canada, L3T 7Z3

Computer Talk Global Corp.

8770 West Bryn Mawr Avenue, Suite 1300
Chicago, Illinois 60631

CONFIDENTIAL INFORMATION

01. Scope of Application

This policy governs ComputerTalk's practices concerning collecting, protecting, managing, and disposing of customer end-user data, which may include personal information arising from using ComputerTalk's PCI DSS and SOC 2-compliant production Cloud Services Environment. It also identifies the distinct accountabilities of the customer and ComputerTalk under the third-party commercial relationship between the customer and ComputerTalk, with particular attention paid to privacy legislation accountabilities. The use of "ComputerTalk" refers to Computer Talk Technology Inc. and Computer Talk Global Corp.

02. Overview

Customers, either directly or through ComputerTalk's channel partners, engage ComputerTalk to design and provision cloud-based technical communications solutions that support specific contact management functions and business processes ("solution" or "customer solution"). This policy is specifically focused on the privacy of persons who either interact with the customer solution intentionally ("end-user" or "customer end-user") or persons whose information is made available to or introduced into the solution by the customer. ComputerTalk, in our role as a third-party supplier, fundamentally understands our accountabilities to secure and protect all end-user data which we process and hold on a customer's behalf through the use of the solution ("solution data" or "customer solution data"). Such data may contain sensitive information, such as payment card or personal information, and be subject to industry standards (in the case of payment card information, PCI DSS) or government legislation (in the case of personal information, FIPPA, PHIPA, or other privacy legislation including GDPR). Our commitment to protecting customer data is reflected in the security standards maintained, security technology deployed, formalized information security policies, operational practices, and ongoing annual comprehensive third-party validation.

03. Privacy vs. Confidentiality

Privacy applies to personally identifiable information (e.g., a person's name, contact information, identification numbers, financial information, medical or health information, as defined in the applicable legislation) which may be captured by a customer solution (e.g., contact records) or otherwise made available or introduced into the solution data environment through the actions or direction of the customer (e.g., customer data integrations such as CRM and web services or import of outbound dialling contact files).

In contrast, confidentiality concerns and applies to commercially sensitive information exchanged between customers and ComputerTalk from communications and transactions arising from a business relationship. Non-disclosure agreements, confidentiality statements, and legal stipulations in the agreements executed define and formalize the business relationship and are covered under ComputerTalk's *Cloud Services Confidentiality Policy*.

04. Separation – Cloud Services and Corporate Network

ComputerTalk's Cloud Services Environment is PCI DSS and SOC 2 compliant and has physical and network separation from ComputerTalk's corporate network. Access from our corporate network to our Cloud Services Environment is through remote access technology and is strictly limited to authorized technical personnel whose job function requires such access. The separation of environments ensures that all customer solution data, including customer end-user data, handled by a customer cloud service solution is protected under a rigorous security standard from internal and external threats, as detailed in ComputerTalk's *Information Security Policies* and the operational processes extending from that policy. Further, ComputerTalk does not engage with any customer to provide live contact response services or third-party staffing.

05. Customer Solution Data – Ownership and Access

The customer owns all customer data, including personal information, collected and stored within ComputerTalk's Cloud Services Environment. ComputerTalk does not access customer data unless specifically authorized by the customer to address documented service performance issues. Then only those records specified by the customer are used as a last resort for troubleshooting. It is ComputerTalk's obligation to provide secure storage of such information under a contractual agreement or as otherwise authorized by the customer.

06. Compliance With Privacy Legislation

The customer is accountable to its end-users, as applicable, to fulfill and respond to privacy legislation requirements under which it operates. In our limited role as a third-party service provider, ComputerTalk, as detailed in this policy, supports the customer in meeting its privacy obligations.

07. Consent to Gather Personal Information

Consent to collect personal information is a matter between the customer and its end-users, with no direct involvement from ComputerTalk. For clarity, the customer is accountable for and must address all issues concerning end-user consent, including, for example, notices that interactions may be recorded, archived, or further processed. It is not incumbent on ComputerTalk to further validate consent issues with the customer or end-user in the ordinary course of business.

08. Interaction With End-Users

Under no circumstance shall ComputerTalk interact with any end-user. All services are provided by ComputerTalk as if the customer is providing the service exclusively for business purposes. On its part, the customer shall not refer any of its end-users to interact with ComputerTalk.

09. Data Encryption

Except for the inbound call leg between the carrier and ComputerTalk's session border controller, all data path connections are encrypted internally and externally, allowing secure end-to-end trusted endpoint data connections between ComputerTalk's cloud infrastructure, the customer network, or other third-party services that are incorporated into a customer solution with the approval of the customer. Within our secure Cloud Services Environment, contact records are encrypted using encryption technologies native to the local dedicated mass storage solution (SAN or disk farm), cloud-based storage (Cohesity), or a combination of the two storage solutions. SQL encryption is used for all database records.

10. Platform Standard Data Capture

The ice Contact Center platform captures data across multiple contact modalities (e.g., voice, messaging, email), including a collection of certain information tied to all handled contacts. The following data may be collected through standard functionality (depending on enabled contact modalities):

a) System configuration information that the customer supplies and manages (e.g., telephone numbers, hours of business, agent names, etc.)
b) End-user contact routing information (e.g., telephone number, email address, etc.)
c) Contact transaction records (e.g., call recordings, screen recordings, email threads, messaging, or chat history) may contain personal information depending on the content of a conversation

Appendix A details the forms of data collected by ice as a platform on a default basis. Knowing what data is collected and why, where it is stored, when it is erased, and how a customer might manage certain forms of information facilitates data privacy assessments and decisions.

11. Sensitive Data Collection

Under some circumstances, the information generated through standard functionality, within the context of *who* is collecting such information, can potentially meet the threshold of personally identifiable information. Further, a customer solution may systematically process and hold personal or other sensitive information as a function of customer business requirements. If there is a reasonable expectation that the solution will routinely capture sensitive personal information, the customer is accountable for identifying this during the pre-sales process, and solution design discussions must be undertaken to understand and adequately account for special design requirements and limitations. Any such exceptional data handling requirements must be part of the solution documentation and meet ComputerTalk's sensitive data processing stipulations as applicable.

12. Storage of Customer Data

On a default basis, voice recordings are archived in the Cloud Services Environment for 90 days with backup to an encrypted cloud service. After 90 days, voice recordings are purged. Email records are retained for one year. For other contact modalities (e.g., webchat), retention of contact records is optional. All retention intervals are configurable. In some cases where sensitive information is captured by a customer solution (Section 11), it is recommended that no storage of such sensitive information be considered, or a customer or third-party storage solution be provided which allows data at rest to be encrypted and, as needed, retained for extended archival periods. The customer also has the ability, through iceJournal, to delete or export individual contact records. If mass removal of a customer's end-user contact records is required, ComputerTalk will process any such request through the Help Desk.

13. Information Security Certification

As a requirement of providing services for some of our customers whose solutions handle payment card data, ComputerTalk's cloud service infrastructure is PCI DSS compliant, validated by a current Attestation of Compliance renewed annually. ComputerTalk undergoes an annual security review through a process conducted by third-party qualified security analysts, including our *Information Security Policies*, validation of operational process controls, penetration tests, direct inspection, evidence-based investigation, and a threat-risk assessment. Dedicated to the rigorous protection of payment card data, ComputerTalk extends that protection to all customer data.

ComputerTalk also has SOC 2 Type 2 certification, extending our third-party certifications to validate our organizational commitment to rigorous information security practices.

14. Staff Awareness and Commitment

Secure handling of all customer data is a formal requirement and part of the established professional culture of ComputerTalk and is reflected in our *Information Classification Standard*. On an annual basis, all employees are required to review our *Staff Handbook - Cloud Services Information Security* and sign an attestation regarding the secure handling and sensitive nature of the data we handle and a commitment to take urgent action should they become aware of any potential compromise of such data.

15. Data Breach Response

As part of our overall security position, ComputerTalk maintains 24/7 active security measures, including monitoring, logging, and active notification of any unusual and potentially malicious activity. If ComputerTalk detects potential malicious activity, a formal security incident response plan is triggered. If a malicious attack is identified and the scope and impact of the attack are confirmed, ComputerTalk advises customer-designated contacts who have the authority to address data privacy-related issues within 72 hours.

16. Third-Party Access

ComputerTalk does not share customer data with a third party unless specifically authorized by a customer, including third-party services incorporated into a customer solution. Any access to our data environment by third parties engaged in technical support is performed through secure remote access technology, supervised by one of our staff at all times, strictly adhering to ComputerTalk's *Information Security Policies*.

17. Actions on Termination of Services

Within 30 calendar days of termination of services, unless otherwise requested by the customer, all information collected through the provision of services is securely deleted along with all other solution components dedicated to the customer's services, including website(s), configuration data, or other data associated with those services. Our change management process performs this work to ensure service termination actions.

Appendix A – Contact Information Collected on a Default Basis by ice

This document details the forms of data collected by ice as a platform on a default basis. Knowing what data is collected and why, where it is stored, when it is erased, and how a customer might manage certain forms of information facilitates data privacy assessments and decisions. Additional information may be captured on a customer-specific solution basis (custom data capture) that is beyond the scope of this document.

01. Contact Detail Record

The contact detail record (CDR) represents events that happen during contact and is captured for all interactions with ice. These records may include personal data, such as:

a) Originating phone number and display name (received from the voice carrier) for voice calls
b) Email address and email display name for emails
c) User-provided email address and name for webchats
d) Originating identity for social media interactions (e.g., Facebook profile ID)
e) Originating phone number and display name for SMS contacts
f) Phone number or email address of an external transfer out of the ice contact center platform

In addition to this information, a CDR may contain user data, a data field used by agents and applications to append extra information to the contact. The use of this data field is application-specific and should be considered as part of a customer implementation. CDR data is captured and retained for the following reasons:

a) Support and troubleshooting: Retention of carrier data can be used to troubleshoot voice quality and messaging connectivity issues in the environment.
b) Statistics and reporting: ice provides various statistical data to customers on contact patterns, including tracking interactions from particular users or endpoints.
c) Service tracking: ice provides tools for users to search for previous interactions with the system based on the contact originator or destination, which allows them to follow up on previous interactions.

By default, CDR data is stored for 375 days, although this is configurable by individual customers. After expiry, the data is deleted. CDR data is required for the normal operation of the ice platform, and customers should reflect this data collection in their privacy policies.

Upon request, a data subject's CDR data can be exported by providing copies of the CDR reports. If a data subject wishes to delete any CDR data, the request can be forwarded to ComputerTalk in writing via our Help Desk. Removal of CDR data entails anonymizing any identifiable fields listed above, which will remove the ability to locate individual contacts in iceJournal and CDR reports. Aggregated statistical data will remain since it contains no personal data.

02. Diagnostic Logs

The data stored in the CDR is also mirrored in the diagnostic logs on ComputerTalk's servers. ComputerTalk's Customer Support and Product Engineering personnel use the data in these logs for support and troubleshooting. This data is retained for 30 days by default, after which it is deleted.

03. Call Recordings

As an optional feature, calls processed by ice can be recorded. The exact purpose of these call recordings is customer-specific. The customer should disclose the purpose for recording to the end-user (e.g., as a broadcast message during the contact routing process). Such disclosure should include whether recordings may be transcribed or used for research or marketing purposes, training, and legal compliance. Recordings are retained for 90 days by default, but retention periods may vary. A recording privacy feature in ice can be invoked to suspend some or all of a call recording selectively to avoid recording sensitive data.

If a data subject requests that an individual call recording be deleted, a customer administrator may do so via iceJournal. Requests for bulk deletion should be submitted in writing to the ComputerTalk Help Desk. Deletion of a call recording does not immediately delete CDR data associated with the recording. If a user requests a copy of a recording, one can be exported via iceJournal by a customer administrator.

04. Screen Recordings

As an optional feature, agent desktops can be recorded by ice. This video recording will contain some or all of an agent's desktop contents while they are associated with a contact. The contents of this screen recording may include any of the CDR data and the contents of other in-scope applications on the agent desktop. A recording privacy feature in ice can be invoked to suspend some or all of a screen recording selectively to avoid recording sensitive data.

If a data subject requests that an individual screen/call recording be deleted, a customer administrator may do so via iceJournal. Requests for bulk deletion should be submitted in writing to the ComputerTalk Help Desk. Deletion of a screen recording does not immediately delete CDR data or voice recordings associated with the screen recording. If a data subject requests a copy of a recording, one can be exported via iceJournal by a customer administrator.

05. Email Transcripts

Emails handled by ice are captured and retained, including the entire body of all messages, replies, and attachments, in addition to the CDR data specified above. The email content is stored as a requirement of the ice platform while awaiting a response from an agent, allowing emails to be rerouted to multiple agents as required. Once an email interaction is completed, the email contents are retained by ice for later retrieval through iceJournal. By default, emails are retained for one year, although this retention period can be modified based on customer requirements.

If a data subject requests that an individual email transcript be deleted, a customer administrator may do so via iceJournal. Requests for bulk deletion should be submitted in writing to the ComputerTalk Help Desk. Deletion of an email transcript does not immediately delete CDR data associated with the recording. If a user requests a copy of an email transcript, one can be exported via iceJournal by a customer administrator.

06. Chat/Messaging Transcripts

As an optional feature, messaging conversation transcripts can be stored by ice. These include web chat, Skype and Microsoft Teams IMs, SMS, Facebook, Twitter, and other text-based messaging channels. Unless expressly excluded, these transcripts include all message contents sent between the data subject and the contact center, including those with workflows or bots. To avoid recording sensitive data, a recording privacy feature can be invoked to selectively suspend some or all of a messaging transcript.

If a data subject requests that an individual messaging transcript be deleted, a customer administrator may do so via iceJournal. Requests for bulk deletion should be submitted in writing to the ComputerTalk Help Desk. Deletion of a messaging transcript does not immediately delete CDR data associated with the recording. If a user requests a copy of a messaging transcript, one can be exported via iceJournal by a customer administrator.

07. Other Locations Data May Be Stored

Independent of the ice platform, the personal data of a data subject may exist in other places. These locations are out of ComputerTalk's control, and ice's data purging policies do not apply to them:

a) Calls or IMs routed via a PBX may have CDR data of their own. For example, caller phone numbers may appear in the call history of agent devices.
b) Email agents receive a copy of any queued emails in their mailboxes, and ice's email purge policies do not extend to these mailboxes.
c) Agents on Skype for Business or Microsoft Teams may have transcripts of messaging conversations stored in their accounts.

08. Customer-Specific Data

This document only covers data captured by the ice platform and is intended to be used as a privacy policy supplement for ComputerTalk's customers. Other personal data collected as part of an application should also be considered for consent, protection, erasure, and export, including CRM systems, custom databases, workforce management systems, and speech or text analytics.