Cloud Services Privacy Policy

Customers engage ComputerTalk to design and provide cloud-based technical communications solutions supporting specific contact management functions and business processes. This policy specifically focuses on the privacy of persons who intentionally interact with the customer solution 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 we process and hold on a customer's behalf through the use of the solution. 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.

Privacy applies to personally identifiable information (PII) (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 or otherwise made available or introduced into the solution data environment through the actions or direction of the customer. 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 authorized by the customer for troubleshooting purposes under a documented incident. Similarly, customer data will only be shared with a third party under conditions specified by the customer as part of the services provided by ComputerTalk. It is ComputerTalk's obligation to provide secure storage of such information under a contractual agreement or as otherwise authorized by the customer.

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 validate consent issues with the customer or end-user further in the ordinary course of business.

Under some circumstances, the information generated through standard functionality, within the context of who is collecting such information, can 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.

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

1-800-410-1051 1-905-882-5000
1-905-882-5501
www.computer-talk.com

Any such exceptional data handling requirements must be part of the solution documentation and meet ComputerTalk's sensitive data processing stipulations as applicable.

ComputerTalk meets and maintains industry-standard security across its entire cloud service infrastructure. ComputerTalk undergoes annual evidence-based security reviews (ISO 27001:2022, PCI DSS, and SOC 2 Type 2) conducted by third-party qualified security analysts, including our *Cloud Services Information Security Policies*, operational process controls, penetration tests, direct inspection, and a *Cyber Security Assessment*.

Securely handling all customer data is a formal requirement and part of ComputerTalk's established professional culture. Every year, all staff must 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.

Computer Talk Technology Inc.

Computer Talk Global Corp.

December 2024