

## Cloud Services Privacy Policy

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 that we process and hold on a Customer's behalf through the use of the Solution ("Solution Data" or "Customer Solution Data"). Our commitment to protecting customer data is reflected in the security standards we maintain, the security technology we deploy, the formalized information security policies, the operational practices, and the 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 specifically authorized by the Customer to address documented service performance issues, and 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.

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, information generated by standard functionality, in the context of who is collecting it, can meet the threshold for PII. 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 documented in the Solution and meet ComputerTalk's sensitive data processing requirements, as applicable.

As a requirement for providing services to 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 (AOC) that is renewed annually. ComputerTalk undergoes an annual security review conducted by third-party qualified security analysts, including validation of operational process controls, penetration tests, direct inspection, and evidence-based investigation. Dedicated to the rigorous protection of payment card data, ComputerTalk extends that protection to all customer data. ComputerTalk also holds SOC 2 Type 2 and ISO 27001:2022 certifications, further validating our organizational commitment to rigorous information security practices.

The secure handling of all customer data is a formal requirement and part of ComputerTalk's established professional culture. Every year, all staff must review our [Cloud Services Information Security Policies](#) and [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.

March 2026