CLOUDTALK

WELCOME TO THE

CloudTalk Security Whitepaper

In this document, you'll gain a comprehensive understanding of our approach to security at CloudTalk, including the policies and measures we have in place to protect your data and ensure the reliability of our services.

For more information on our data privacy compliance, please visit our Privacy Center.

CLOUDTALK

You can navigate this whitepaper through the following sections:

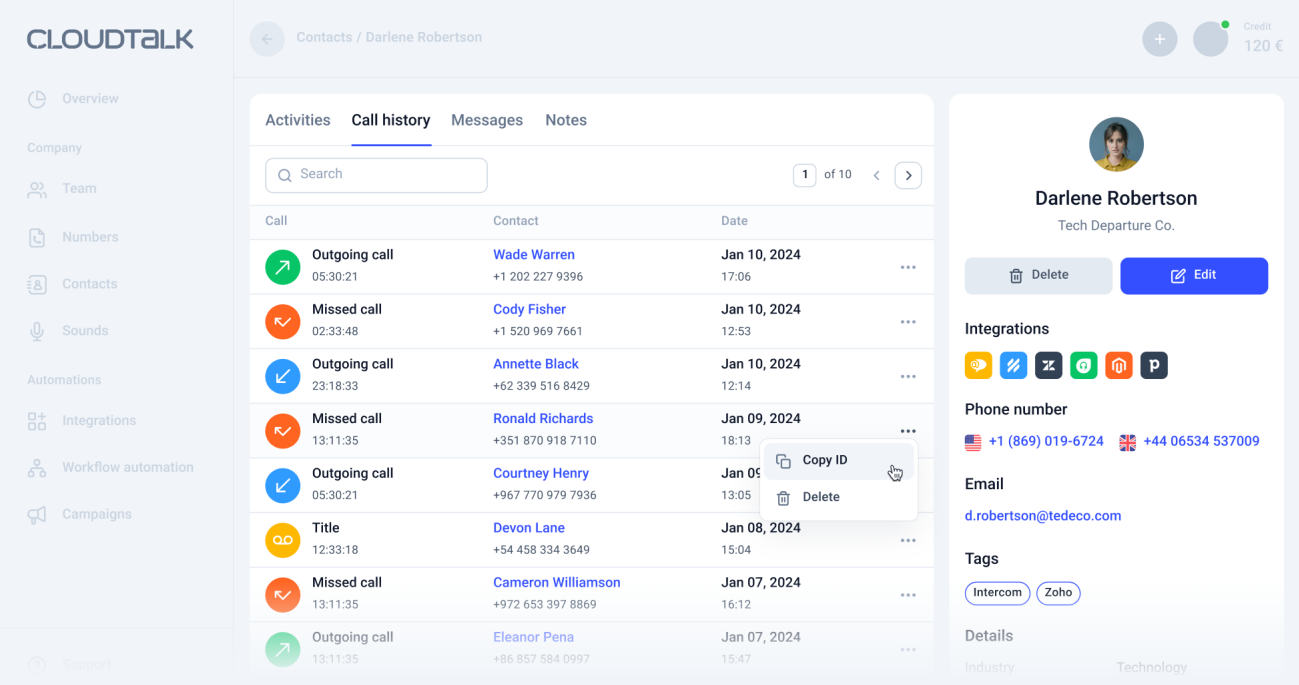
CLOUDTALK

About CloudTalk

About CloudTalk

CloudTalk is the world's most capable AI business calling software for sales and support teams to seamlessly connect with their customers and make customer experience their greatest competitive advantage. Since 2016, CloudTalk has been shaping the phone industry with ready-made integrations, advanced user-friendly customization and revolutionary workflow automation options.

CloudTalk is offered as a Software-as-a-Service (SaaS) solution and is accessible via desktop app, mobile app (iOS & Android), and browser (phone.cloudtalk.io, my.cloudtalk.io and dashboard.cloudtalk.io).



CLOUDTALK

Our Security Framework

Our Security Framework

Security and data privacy are ingrained in the very fabric of our operations at CloudTalk. We recognize that the trust our clients place in us is built upon our ability to protect their sensitive information, ensure the confidentiality of their communications, and comply with the ever-evolving landscape of data protection regulations.

Information Security: SOC 2 and ISO 27001 Compliance

As we progress toward concluding our SOC 2 Type 2 audit in 2025, we have already completed a SOC 2 Type 1 audit and ISO/IEC 27001 certification. This demonstrates our commitment to meeting rigorous international standards for information security.

Data Privacy: GDPR, CCPA, HIPAA and PCI DSS Compliance

We are fully compliant with key data privacy regulations, including the General Data Protection Regulation (GDPR) in Europe and The Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA) in the United States. These frameworks are integral to our operations, ensuring the highest standards of care, transparency, and accountability in handling personal data. We also comply with the PCI DSS Merchant requirements through the Self-Assessment Questionnaire (SAQ A 4.0).

If you are a HIPAA-regulated organisation and need to sign the Business Associate Agreement (BAA) with us, please contact our sales.

Our Security Framework

Continuous Monitoring and Improvement

Security is not a one-time effort but an ongoing commitment. CloudTalk continuously monitors its security posture, regularly reviews its policies and procedures, and updates them as necessary to respond to new threats and changes in the regulatory landscape. This commitment to continuous improvement is a core component of our compliance and our broader security strategy.

CLOUDTALK

People Security

People Security

Hiring

We prioritize hiring candidates who not only excel in their skills but, more importantly, align with our core values. We conduct a rigorous vetting process, including thorough reference checks, to ensure we build a team with strong integrity that upholds our commitment to our customers.

Training and Awareness

Every new hire undergoes comprehensive security training during onboarding, reinforced with annual refresher courses. Our policies are written in clear, straightforward language, emphasizing business implications, and are easily accessible to all employees. We tailor our training to individual teams to ensure the highest level of engagement and understanding.

Access Management

Our access management policy includes:

Least-Privilege Access: Employees are granted the minimum level of access required to perform their job functions, reducing the risk of unauthorized data exposure.

VPN, Single Sign-On (SSO) and Two-Factor Authentication: All internal systems are accessible via VPN only. To enhance security and streamline access, we implement SSO and 2FA wherever possible.

Onboarding and Offboarding: Access rights are carefully managed during employee onboarding and promptly revoked during offboarding to prevent unauthorized access by former employees.

Segregation of Duties: We enforce segregation of duties to prevent conflicts of interest and reduce the risk of fraud or error.

Periodic Review of Access: At least yearly audits are conducted to review access permissions, ensuring that they remain appropriate and that any unnecessary access is promptly removed.

People Security

Confidentiality Clauses

Every employee and contractor at CloudTalk signs confidentiality agreements as part of their contract. These clauses are designed to safeguard sensitive information and reinforce our commitment to data privacy throughout and beyond their employment.

Endpoint Security

All company devices are secured by a comprehensive endpoint management system that enables remote control and asset management. This includes features such as device tracking, remote wipe, full encryption, enforced screen lock and automatic software updates.

Physical Security

CloudTalk operates as a remote-first company, prioritizing security through robust endpoint and access management. Our physical premises are located in co-working spaces with centrally controlled and logged access via physical keys or mobile apps. These spaces are monitored by CCTV and safeguarded by on-site security and reception staff to prevent unauthorized access. Additionally, comprehensive emergency procedures are in place to address incidents effectively and ensure the safety of our employees and operations. No servers or data storage are housed within our physical premises.

CLOUDTALK

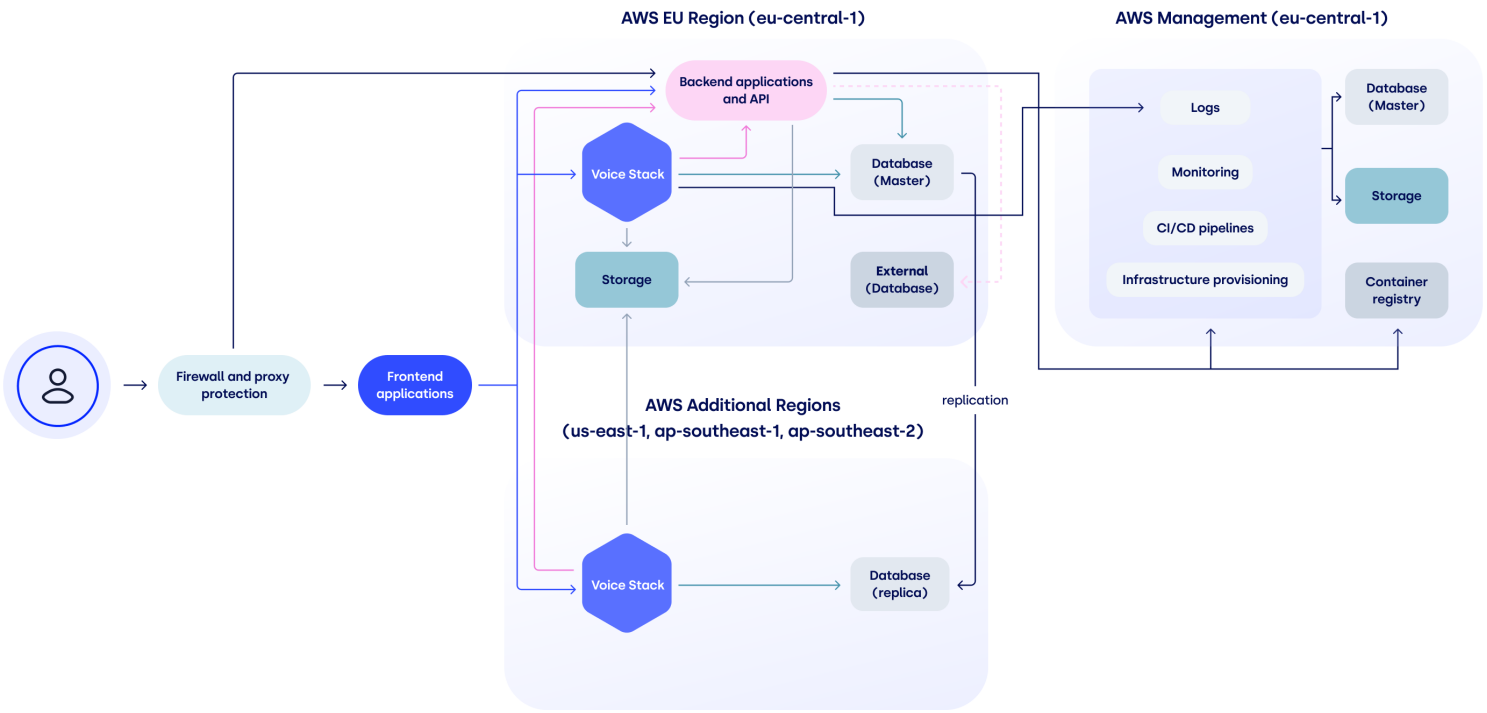
Infrastructure & Data

Infrastructure & Data

Data Hosting and Location

For our cloud infrastructure, we rely on Amazon Web Services (AWS), one of the most secure and reliable cloud service providers in the world. AWS offers a broad range of security features. Their data centers are monitored by 24×7 security, biometric scanning, video surveillance and are continuously certified across a variety of global security and compliance frameworks. Read more at https://aws.amazon.com/security/

All our data is stored across four AWS regions: Frankfurt (eu-central-1), Northern Virginia (us-east-1), Singapore (ap-southeast-1), and Sydney (ap-southeast-2). Leveraging multiple AWS regions, redundant infrastructure and replica databases enhances our disaster recovery capabilities, ensuring high availability and low call latency.
Call recordings are stored in the EU only.



Infrastructure & Data

Data Transfers

We work exclusively with established and respected sub-processors who adhere to the highest security standards and are fully GDPR compliant. The majority of our U.S.-based sub-processors are also part of the EU-US Data Privacy Framework (DPF). We have signed Data Processing Agreements (DPAs) with Standard Contractual Clauses (SCCs) for each sub-processor to ensure compliance with data protection regulations.

For data transfers to the U.S., we have conducted a Transfer Impact Assessment (TIA), which is available upon request. A comprehensive list of our sub-processors is accessible at https://cloudtalk.io/sub-processors.

Multi-Tenant Environment

CloudTalk runs in a multi-tenant cloud environment. Tenants are segregated within the application logic, in line with standard practices for modern SaaS solutions. All data access is authenticated, and the application logic ensures that only data belonging to the authenticated company is provided to the requesting party.

Encryption – in Transit and at Rest

All data transmitted to and from CloudTalk is encrypted using 256-bit encryption. Our API and application endpoints are TLS/SSL-only and consistently achieve an "A+" rating on Qualys SSL Labs tests. This ensures that we use only strong cipher suites and have advanced security features like HSTS and Perfect Forward Secrecy fully enabled. For encryption at rest, recordings are secured using SSE-S3, while other data is encrypted using AWS EC2 drive encryption with AWS KMS. All keys are managed by selected members of the IT security team.

All passwords are encrypted using an advanced one-way hashing algorithm and are never stored for internal purposes. Additionally, all phone calls made via the WebRTC protocol are automatically encrypted, while those made through the SIP protocol can be encrypted using TLS.

Infrastructure & Data

Data Backup

Backups are continuously maintained with multiple live replicas, ensuring at least one primary and two replica copies are always available. We retain 30 days of backups for each database, with daily snapshots stored in a secondary service, and hourly snapshots for Call Data Records. Full redundancy guarantees data safety in case of a system failure. For customers needing additional backups, CloudTalk offers export features and public APIs to easily sync data with other systems.

Data Retention

Clear data retention policies are crucial for minimizing the risk of sensitive information being compromised. By default, CloudTalk retains your data for as long as your account remains active and for 6 months after account closure. Following this period, the data is automatically removed from our daily backups within 1 month. This retention policy helps prevent complications in cases of temporary account closures, such as those caused by expired payment methods or other issues. Call Detail Record (CDR) data is stored indefinitely to meet legal obligations.

If you wish to have any data permanently deleted from your account, our customer support engineers can promptly handle this request using our purpose-built internal tools.

Network Security

CloudTalk's network is divided into public and private subnets to ensure clear separation of resources. We use firewalls to tightly control traffic between these segments, deploy Intrusion Detection Systems (IDS) to monitor and respond to any suspicious activity, and implement DDoS protection to defend against distributed denial-of-service attacks, keeping our infrastructure secure.

CLOUDTALK

Application Security

Application Security

Vulnerability and Patch Management

We maintain a comprehensive vulnerability management policy to ensure the security and stability of our software products. This policy emphasizes the timely identification, assessment, prioritization, and remediation of vulnerabilities across all development teams. Vulnerabilities are categorized by severity, with defined SLAs for remediation—from immediate fixes for critical issues to structured timelines for lower-risk vulnerabilities. Our approach integrates automated scans, manual reviews, penetration testing, bug bounty program and external reports, ensuring a holistic identification process. Accountability is enforced through clear ownership, regular sprint reviews, and escalation processes, ensuring that vulnerabilities are resolved efficiently and in alignment with our commitment to robust security practices.

Penetration Testing

CloudTalk conducts annual penetration testing through an independent third-party security firm. Vulnerabilities identified are categorized, prioritized, and swiftly addressed. The findings guide our mitigation and remediation efforts, ensuring continuous improvement. Importantly, no customer data is exposed during testing. Reports are available under NDA.

Monitoring

CloudTalk maintains its own continuous monitoring services in order to ensure control and availability of customer data, including database monitoring, application monitoring and error reporting and monitoring.

CLOUDTALK

Business Continuity

Business Continuity

Availability and Regional Zones

Our infrastructure, hosted on AWS with accessibility of minimum 99.993%, is distributed across multiple availability zones and regions, guaranteeing continuity even in the event of a localized failure or disaster. We adhere to secure data storage practices, using replicas redundant infrastructure and regular backups, and we follow the AWS Well-Architected Framework to maintain high availability and reliability.

Incident Management

Our Incident Management Policy enables us to respond swiftly and effectively to security incidents. The program includes clear guidelines that define procedures, roles, responsibilities, and contacts. Trained Incident Commanders lead our response efforts, with incidents categorized into four severity levels. Post Mortems are conducted to identify preventive actions, and for high-severity incidents (P1), a Root Cause Analysis (RCA) is published within two days, with RCAs available on request for P2 incidents. In the event of a security incident involving client data, we promptly notify affected clients through their designated Customer Success Manager (CSM) or our support team. Additionally, we have a Data Breach Response Plan in place to ensure compliant resolution of such incidents.

Service availability updates are regularly posted on our status page at https://status.cloudtalk.io/, where clients can also subscribe to notifications for scheduled outages. For any concerns or incidents, please contact us directly at security@cloudtalk.io.

Disaster Recovery

We have implemented a comprehensive disaster recovery plan to safeguard our operations and ensure business continuity in the event of unexpected disruptions. This plan is rigorously tested through annual disaster recovery drills to validate its effectiveness and identify areas for improvement. Our infrastructure is specifically designed with disaster recovery principles in mind, incorporating redundancy, failover mechanisms, and geographically dispersed data centers to minimize risks.

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are clearly defined within our plan to set precise benchmarks for system restoration and data recovery. These objectives are thoroughly tested and evaluated during each drill to ensure that we can meet or exceed our commitments. By proactively preparing and regularly testing our disaster recovery protocols, we maintain a high level of resilience and readiness, minimizing potential downtime and ensuring seamless continuity of services for our customers and stakeholders.

CLOUDTALK

Vendor Management

Vendor Management

We adhere to our Vendor Management Policy, which outlines clear processes for approving new vendors and managing changes. All new vendors undergo security assessments, and we regularly review the security practices of vendors handling sensitive data. We collaborate exclusively with reputable and well-established sub-processors who uphold the highest security standards and maintain full compliance with GDPR. We have signed Data Processing Agreements (DPAs) with Standard Contractual Clauses (SCCs) for each sub-processor to ensure compliance with data protection regulations.

CLOUDTALK

Application Security & Data Privacy Features

Application Security & Data Privacy Features

We are committed to empowering your organization's compliance and safeguarding your data privacy. With CloudTalk, you don't have to worry about compliance—we build it directly into our features. Our comprehensive security tools are designed to ensure that your company meets regulatory requirements seamlessly while using our services. Below is an overview of the essential security features we provide:

Authentication: Supports Google, Okta, Azure, OneLogin, Keycloak, Salesforce or standard email and password authentication.

Two-Factor Authentication (2FA): Can be enabled within supported SSO solutions for an extra layer of security.

Password Requirements: Passwords must be 10 to 50 characters long and include at least one lowercase letter, one uppercase letter, one number, and one special character.

Role-Based Access Control: CloudTalk offers user management with different roles, each having distinct access rights:
Admin - the highest level of access
Supervisor - can manage groups of agents based on admin settings
Agent - can perform actions within their group based on admin settings
Analyst - can view and analyze statistics

International Calls: Enables you to specify the countries from which your agents can make calls, with the option to set a maximum daily credit limit for each agent.

Action Logs: Full audit logs of actions related to Contacts, Calls, or Recordings are accessible through the Admin interface. These logs are encrypted and protected against tampering.

Application Security & Data Privacy Features

Features Supporting Your GDPR and CCPA Compliance

Delete Contacts („Right to be Forgotten"): You may delete contacts upon a customer's request at any time. Deleting a contact removes all related data, except for the calls and call recordings. These calls will no longer be linked to the contact and can only be identified by phone number. Contacts can also be deleted seamlessly using our API.

Delete Call Recordings: You can delete customer communications on demand. Once deleted, the recording is permanently removed from all our services.

Remove Data from Integrations: When specific data needs to be deleted from an integration (e.g., specific orders) while retaining other data, you can use our API to delete those items automatically, or delete individual records directly through the CloudTalk interface in contact details.

Access to Recordings: You can control whether each agent can access call recordings and whether they can only play or download them. These settings help improve the security of your data.

Access to personal data:
You can hide contact details from certain user roles.

Exporting Customer Data („Right of Portability"): Customers are listed as „Contacts" in CloudTalk. You can easily export the entire communication history with a particular customer to an Excel file and provide it to the customer if necessary. Data can also be exported using our API.

Blacklist / Unsubscribe Contacts: You can block inbound and outbound calls to specific numbers.

Pause and Resume Call Recording: Agents are able to pause recordings during calls to prevent capturing sensitive information.