SECURITY AND PRIVACY WHITE PAPER

Poly One Touch Dial

Part 3725-85485-001

Version 02

April 2020

Introduction

This white paper addresses security and privacy related information regarding Poly One Touch Dial (OTD) Cloud Service.

This paper also describes the security features and access controls in Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the Poly One Touch Dial service, and the location and transfers of personal and other customer data. Poly will use such data in a manner consistent with the Poly Privacy Policy, and this white paper which may be updated from time to time. This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper will be available on Poly's website.

The Poly One Touch Dial cloud service enables an endpoint device to join a meeting by simply clicking a "join" button on the device without the need to dial a potentially long string of digits or a URL. The Poly One Touch Dial cloud service can be used as a standalone service or it is often paired with Poly RealConnect cloud service or other third-party conference hosting services providing the convenience of simplifying how an endpoint joins a meeting.

Note: This white paper only addresses the Poly One Touch Dial cloud service. Poly Global Services also offers the Poly One Touch Dial App, which is a software application that is installed as a web service on customer premises. More information about the Polycom One Touch Dial App may be found here.

Security at Poly

Security is always a critical consideration for a cloud-based service such as Poly One Touch Dial. Poly aligns with ISO/IEC 27001:2013 for our Information Security Management System (ISMS). ISO/IEC 27001 is the most widely accepted international standard for information security best practices and you can be reassured that Poly has established and implemented best-practice information security processes.

Product security at Poly is managed through the Poly Security Office (PSO) which oversees secure software development standards and guidelines. The Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013 and OWASP for application security. Guidelines, standards and policies are implemented to provide our developers with industry approved methods for adhering to the Poly Product Security Standards.

Secure Software Development Life Cycle

Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development process. Every phase of the development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

Change Management

A formal change management process is followed by all teams at Poly to minimize any impact on the services provided to the customers. All changes implemented for the Poly One Touch Dial cloud service go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production. While emergency changes are processed on a much faster timeline, risk is evaluated and approvals are obtained from stakeholders prior to applying any changes in production.

Privacy by Design

Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions, and processing of personal data and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, Poly considers the right to data protection with due regard.

Secure Deployment

The Poly One Touch Dial cloud service supports two deployment topologies. In support of Poly endpoints, Exchange Web Services is used to provide the calendar to the endpoint. For third-party endpoints, the Poly Cloud Relay is deployed on-premises to push calendar events to the endpoint through the endpoint's native API.

Calendar connections over Exchange Web Services support TLS v1.2. Older versions of TLS are available to support legacy endpoint models. Consult the Administrator's Guide for detailed information about configuration options.

For customers that have opted to deploy Poly Cloud Relay, communication of calendar events from the service to the on-premises virtual appliance is encrypted using TLS v1.2 and delivered over an AMPQ message bus. Subsequent delivery of calendar events from Poly Cloud Relay to the endpoint is over the customer's internal network.

The Poly One Touch Dial cloud service ensures that your communications are secure and does not record or capture calendar events. As stated above, calendar events that are transported between the service and the customer's endpoint are encrypted using TLS.

All traffic transported between the Poly One Touch Dial cloud service and Microsoft O365, Microsoft Exchange on-premises and Google as calendar providers is always encrypted.

User Authentication

The Poly One Touch Dial cloud service supports integration of enterprise authentication providers via the OAuth2 standard.

With OAuth2, the Poly One Touch Dial cloud service can securely integrate with enterprise authentication providers and thereby authenticate enterprise users without ever having access to their credentials. Users enter credentials only into the authentication provider's own sign-in page. Poly One Touch Dial then receives access tokens from the authentication provider that grants limited and controlled access to resources owned by a user.

Note:

- Access tokens are not stored by the cloud service. They are discarded after being used to obtain basic user profile information (user email address, user display name)
- Access tokens have limited lifetimes controlled by the authentication provider
- Refresh tokens are cached for continued calendar access on behalf of the calendare

owner in order to provide ongoing updates to the video endpoint device.

- The cloud service supports the following authentication providers:
  - Microsoft Active Directory Federation Services 3.0 via OAuth2
  - Microsoft Office 365 (Azure AD) via OAuth2

Cryptographic Security

All communication with the Poly One Touch Dial cloud service web portal is encrypted over an HTTPS connection that uses TLS 1.2 with 128 or 256-bit encryption and a 2048-bit key exchange mechanism. Cryptographic cipher suites and modules implemented in the Poly One Touch Dial cloud service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated and leverage the Advanced Encryption Standard (AES-128 and AES-256) cipher suites. Hash strengths supported include SHA-256 and SHA-384.

Disaster Recovery and Business Continuity

The Poly One Touch Dial cloud service is architected to provide high reliability, resiliency and security. The entire service is hosted on multiple geographically distributed Microsoft Azure data centers in the United States, the Netherlands or Australia. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting provider—Microsoft Azure.

During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. Poly tests disaster recovery processes and procedures on an annual basis. We use the results of this testing process to evaluate our preparedness for disasters and to validate the completeness and accuracy of our policies and procedures.

Data Processing

Poly does not access any customer's data except as required to enable the features provided by the service. If you are an individual user and the purchase of the Poly One Touch Dial cloud service has been made by your employer as the customer, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Source From Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Account information	• Email address • Username and password	• Reading calendar information • Display of calendar to device association • Deliver the service • Internal analysis and reporting	Azure
Device Information	• IP address	• Push calendar to video conferencing endpoint • Help customer diagnose technical issues	Azure

Purposes of processing

The primary purposes of processing information by the Polycom One Touch Dial cloud service is to enable an endpoint device to join a meeting by simply clicking a “join” button on the device without the need to dial a potentially long string of digits or a URL. Additional processing of information is for logging and diagnostic purposes and security adjudication.

How Customer Data is Stored and Protected

The Poly One Touch Dial cloud service stores customer data in Azure CosmosDB. Data is encrypted at rest using AES 256. Data may reside in the United States, the Netherlands or Australia.

To learn about how encryption is applied, please visit the following link here.

The Poly One Touch Dial cloud service database server is in an SSAE 16 Type II certified data center in the United States, the Netherlands or Australia that runs dedicated databases and application servers. When the Poly One Touch Dial cloud service database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

Poly may change the location of the Poly One Touch Dial cloud service database server and details of any such change shall be set forth in the latest copy of this white paper available on Poly’s website.

For transferring personal data of EU customers to the US, Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

The Poly One Touch Dial cloud service database and application servers reside in the data center behind a fully patched firewall that is also managed. Access for any services not required by the Poly One Touch Dial cloud service is blocked.

Server Access and Data Security

All customer data sent to Poly is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

All customer data sent to Poly is backed up daily in digital form using the Azure data factory. Normal access controls of authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data during rest and while in transit is encrypted using AES 256.

Servers are in a secure data center, with only authorized staff members having access. The servers are not directly accessible from outside the data center. For details, see here.

Data Deletion and Retention

All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of the Poly One Touch Dial cloud service. All data is self-contained in the database in the data center.

Poly may retain customer data for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. Poly may “anonymize” personal data in lieu of deletion. In cases where anonymization occurs, the process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

Security Incident Response

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact the PSO directly at informationsecurity@Poly.com
The PSO team works proactively with customers, independent security researchers, consultants, industry organizations and other suppliers to identify possible security issues with Poly products and networks. Poly security advisories and bulletins can be found on the Poly Security Center.

Subprocessors

Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third party data processor who, on behalf of Poly, processes customer data. Prior to engaging a subprocessor, Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies Poly's authorized subprocessors and includes their name, purpose, location and website. For questions, please contact privacy@poly.com.

Prior to engagement, suppliers that may process data on behalf of Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

Additional Resources

To learn more about Poly One Touch Dial cloud service, visit our product website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product. You may copy and use this paper for your internal reference purposes only. POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.