SECURITY AND PRIVACY WHITE PAPER

Polycom® Elite Service Overview

Part 3725-86521-001

Version 01

October 2019

INTRODUCTION

This white paper addresses security and privacy related information regarding Polycom® Elite Service. This white paper describes the security features and access controls applied to Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the 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*.

Polycom Elite Service is personalized and proactive support for your Polycom solution.

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, even more so for Support Services.

Poly's delivery of the Polycom Elite Service utilizes the ITIL framework.

Poly's Information Security Management System (ISMS) aligns with ISO/IEC 27001:2013. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers 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 for the implementation of specific security technologies, such as cryptographic controls related to ciphers, protocols, storage, and web services, are intended to provide our developers with industry approved methods for adhering to the Poly Product Security Standards.

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 while also enabling the data controller to create and improve security features.

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 to make sure that data controllers and processors can fulfill their data protection obligations.

DATA PROCESSING

System logs and call detail records can be collected by or sent to Poly. These may contain names, emails, IP addresses, locations.

Customers who contact Poly for technical support are asked to provide contact information.

If you are an individual user and the purchase of a Poly 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.

Personal Data Category	Type of Personal Data	Purpose of Processing
Support and Reporting services	- Endpoint Display Name - User Email Address - User ID - User Phone number - User address/location	- Troubleshooting and support remediation - Provide required reporting

PURPOSE OF PROCESSING

The primary purposes of processing information by the Polycom Elite Service is to provide support and reporting per agreement requirements.

HOW CUSTOMER DATA IS STORED AND PROTECTED

Poly may change the location of the business systems used to process customer information. The 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.

When Poly Elite Services needs to store customer or personal data to provide reporting, the data is processed as follows:

Category	Where it stored and how protected	How long
Reporting Data	Encrypted server in Poly IT environment	13 months or the conclusion of the engagement
Technical Support	Stored in Poly CRMs, stored on sftp	Temporarily held until 90 days after ticket is closed

DATA SECURITY

Computers used to process customer information in the delivery of Polycom Elite Services are protected from malware and viruses, patched in a timely manner and utilize encryption to protect any data stored locally. They adhere to Poly's ISMS requirements for controlled access and follow least privilege and need-to-know principles. When these computers are used remotely, they must authenticate to the Poly network using MFA.

When assets are retired, media is sanitized per the Poly Media Sanitization standards, which is based on NIST 800-88.

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

Poly shares customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is consistent with the *Poly Privacy Policy*.

DATA DELETION & RETENTION

When a customer makes a request for deletion, Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate business purposes or if needed to provide the service to customer. Poly may "anonymize" personal data in lieu of deletion. The anonymization process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (such as 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. *https://support.polycom.com/content/support/security-center.html*

ADDITIONAL RESOURCES

To learn more about Poly services, please visit our 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.