SECURITY AND PRIVACY WHITE PAPER

Poly Lens

Part 3725-86286-001

Version 02

December 2020

Introduction
This white paper addresses security and privacy related information for the Poly Lens 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 Lens 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.

Poly Lens provides an enrolled customer with access to a dedicated web portal which includes device management of Poly conferencing endpoints and basic reporting capabilities. Reports are based on data (including certain personal data of a customer as described below) collected from a customer's Poly endpoints that are configured to send data to Poly. Customer data is automatically uploaded to Poly Lens and accessed via the Poly Lens web portal application using an encrypted tunnel and software module embedded in the endpoints.

Security at Poly
Security is always a critical consideration for a cloud-based service such as Poly Lens. 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 processes. Every phase of 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 Lens 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.

Poly Lens Tunnel
When Poly endpoints are configured to send data to Poly Lens, each endpoint establishes an IoT connection to Poly Lens. To configure available options for sending data, please see the Privacy Guide and Administrator's Guide for the specific endpoint device.

A Poly Lens agent on the endpoint uses device-specific credentials to transmit data to Poly Lens using specific ports. All credentials are encrypted via HTTPS tunnel using TLS 1.2. Data is transported and deposited in the Azure data store, located in an SSAE 16 Type II certified Microsoft data center in the United States. All communication between the endpoint and data store is via the encrypted web socket. Any attempt to monitor the link between the agent and data center servers will only show encrypted data packets instead of cleartext information.

Poly Lens Portal
The Poly Lens web portal processes information that the devices have reported to Poly Lens and then presents it to the user.

The following list describes the secure deployment configuration:

- Secure Device IoT connection
- All packets are encrypted
- The socket connection is encrypted

User Authentication
The Poly Lens portal authentication service supports single sign-on (SSO) and can be integrated with the customer's active directory via OAuth 2, an authentication protocol that allows users to authenticate for Poly Lens using their enterprise credentials without actually sharing their credentials with Poly. Users will use their Office 365, ADFS, or Okta credentials to log into the portal.

Alternatively, users can us Google sign-in to manage the OAuth 2 flow and token lifecycle or create local accounts with email addresses.

Administrators can add additional Poly Lens users by inviting them to a tenant via email. User authentication for Poly Lens can be performed in two ways.

Disaster Recovery and Business Continuity
The Poly Lens service is architected to provide high reliability, resiliency and security. The service is hosted in multiple Microsoft Azure and Amazon AWS data centers in the United States. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting providers —Microsoft Azure and Amazon AWS.

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 but are sometimes

conducted more frequently when there are changes to our infrastructure that warrant new tests. 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.

Cryptographic Security

Data at rest is protected using standard (AES-128 and AES-256) cipher suites as well as hash strengths including SHA-256, SHA-384 and SHA-512.

Poly requirements for cryptographic ciphers include:

- Greater than or equal to 128-bit keys for symmetric ciphers.
- Greater than or equal to 2048-bit keys for asymmetric ciphers and Diffie-Hellman key exchange algorithms.
- Greater than or equal to 256-bit curves for Elliptic Curve Cryptography (ECC).

All communication with the Poly Lens portal web servers and client browsers is over a standard secure SSL connection that encrypts all requests and responses. This is achieved with an HTTPS connection that uses TLS 1.2 with a 256-bit encryption layer using SSL and certificates. This connection is encrypted and authenticated using AES_128GCM with ECDH as the key exchange mechanism.

Transport Layer Security (TLS) between components of the Poly Lens is TLS 1.2 for connections, and versions prior to TLS 1.1 are disabled. TLS compression and client-initiated renegotiation also are disabled. Where implemented, secure server renegotiation is compliant with RFC 5746.

Cryptographic cipher suites and modules implemented in Poly Lens are open (publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated, and leverage the Advanced Encryption Standard.

Daily backup snapshots are automated, encrypted and securely stored. Services are architected for High Availability (HA). Services are built to be fault tolerant within the Azure and AWS data centers and each component is made up of multiple instances.

Data Processing

Poly is the processor of customer data while the customer is the data controller.

Poly group or room conferencing devices automatically send product usage data, device data, call detail records (CDRs) and quality of service data to Poly Lens. To turn OFF data collection, please see the Privacy Guide and Administrator's Guide for your device. Poly personal or desktop devices do not send data by default and must be configured by the device administrator to do so.

Poly has access to customer personal data that is sent to Poly Lens when Poly devices are configured to do so. Customer personal data may also be reported to an internal analytics service used for product improvement purposes. Poly Lens service also collects and processes logs containing:

- Device data (includes details such as type of device, device name, installed software version, etc.)
- CDR data (includes call connection information such as IP addresses, phone numbers, call ID, local and remote call participant names, etc.).

If you are an individual user, and the purchase of Poly Lens 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
Device Administrator and user information	• First/Last Name • User ID • SIP username • SIP alias name • Email address • Password (hashed) • Organization name • Tenant ID	• Authenticate and authorize administrative access to the service • Deliver the service • Reporting • Usage/activity	Auth0, Azure, AWS
Device Identifier Information	• Device ID • Device name • MAC address (for both primary device and paired/ unpaired IP peripherals) • Serial number • IPv4/v6 address • SIP address • MAC address • Display name • System name • System owner • Domain name • Log files • Device geolocation data including time zone • Network identifiers	• Understand how devices are being used in a customer environment • Help customer diagnose technical issues • Collect analytics to improve the technical performance of the customer's UC service • Provide details in support of room or devices issues that require support • Serial number for entitlement	Azure, AWS
Local and Remote Call Participant Information	• Full Call detail record (CDR) • Dial string number • Call ID • Participant names (local and remote) • Participant IP addresses (local and remote)	• Customer identification of specific troubled calls • Short-term, transient use (login)	Azure, AWS

Purposes of processing

The primary purposes of processing information with Poly Lens service is to:

- Enable inventory management—View your devices and manage important information like software versions and device data.
- Perform data analytics—Better understand utilization, performance and call quality.

Personal data is processed for display and reporting purposes only.

How Customer Data is Stored and Protected

Poly Lens stores customer data in Azure and AWS databases. Data is encrypted at rest using AES 256. Data resides in the United States.

The Poly Lens database servers are in SSAE 16 Type II certified data centers in the United States that run dedicated databases and application servers. When the Poly Lens database servers receive data from the customer, it is verified for integrity, processed, and saved in the databases.

Poly may change the location of the Poly Lens database servers 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 Lens databases and application servers reside in data centers behind a fully patched firewall that is also managed. Access for any services not required by Poly Lens 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 secure data centers, with only authorized staff members having access. The servers are not directly accessible from outside the data centers.

Data Deletion and Retention

All information collected from the customer is stored in the databases with the tenant information configured as the access control mechanism. Nothing is transmitted outside of Poly Lens. 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 Lens, 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.