

Privacy Data Sheet

This Privacy Data Sheet describes the processing of personally identifiable information (as defined by the European Union General Data Protection Regulation) (“personal information”), by ThousandEyes’s Software-as-a-Service application as of January 1, 2019. This Data Sheet will continue to evolve as ThousandEyes improves and expands its product offerings. If you would like to receive notifications regarding changes to this Privacy Data Sheet, please contact your account manager or send an email to sales-inquiries@thousandeyes.com.

Product Overview

WEB PLATFORM:

The ThousandEyes web platform is the primary user interface for the ThousandEyes Service, and as such, it stores the login credentials for any users authorized by the customer administrator, including user names, email addresses, and passwords for the purpose of authentication and email delivery. For security audit purposes, user email addresses and their IP addresses are captured in the system and application logs.

CLOUD AGENTS:

Cloud Agents are testing nodes situated in the cloud around the world, operating in over 175 cities and 54 countries. Customer-configured tests running from each node provide performance data which simulates end user experience, gathered from local transit providers and last-mile ISPs. Cloud Agents are generally used to monitor the public internet, but may process personal information if tests configured by the customer include personal information. For example, if a customer wishes to monitor page load times for web application login, the test may include login credentials.

ENTERPRISE AGENTS:

Enterprise Agents are equivalent to Cloud Agents, but are hosted in customer-controlled environments. Customers are able to configure tests to monitor the health of their network infrastructure and the performance of key applications from their networks across the public internet. Enterprise Agents are most commonly installed in branch sites and within data centers to provide a detailed understanding of wide area networks, internet connectivity, and latency. As with Cloud Agents, Enterprise Agent may process personal information if tests configured by the customer includes such information.

ENDPOINT AGENTS:

Endpoint Agents are software testing agents deployed by customers on computers within their organization to help troubleshoot network and application performance. Customer’s administrators configure the tests, which specify the types and sources of information collected by the Endpoint Agents. The test results (e.g., page load time) are uploaded to the customer’s account on the ThousandEyes platform. If so configured by a customer, Endpoint users may also manually record data performance metrics by targeting a specified domain. Endpoint Agent may process the following personal information: end-user computer name, name of logged-in user, IP address, metro area location information derived from the IP address, and any personal information included or resulting from customer-configured tests.

[Remainder of this page intentionally left blank]

The Customer can configure the Endpoint Agent to collect data in four ways:

1. Automatic data collection: The Endpoint Agent will gather performance data associated with the end user's browsing session when the computer is operating within networks selected by customer administrators, and the end user visits a website which is selected for monitoring by customer administrators.
2. Manual data collection: The end user can initiate data collection from within Google Chrome by clicking the ThousandEyes logo in the extension toolbar. While the Endpoint Agent is recording the browsing session, the top of the page will show a banner indicating that ThousandEyes Endpoint Agent is debugging the tab. To stop recording, simply click the ThousandEyes logo in the toolbar, or click the Cancel button on the banner.
3. Scheduled data collection: The Endpoint Agent may be configured to collect data about network and application performance to specified destinations at regular intervals, as defined by the customer's administrator.
4. Instant test data collection: To provide rapid assistance when troubleshooting, a customer administrator can initiate a test immediately. This test will run straight away without waiting for a scheduled event. The data collected is identical to a scheduled test.

ENDPOINT AGENT PULSE:

Endpoint Agent Pulse is typically used by customers to troubleshoot connectivity into unmanaged networks, such as their client sites or employee-owned devices. Customer's administrators configure the tests, which specify the types and sources of information collected by the Endpoint Agent Pulse. The test results (e.g. availability, response time) are uploaded to the customer's account on the ThousandEyes platform. Endpoint Agent Pulse may process the following personal information: end-user computer name, IP address, metro area location information derived from the IP address, and any personal information included or resulting from customer-configured tests.

The customer can configure the Endpoint Agent to collect data in two ways:

1. Scheduled data collection: The Endpoint Agent may be configured to collect data about network and application performance to specified destinations at regular intervals, as defined by the customer's administrator.
2. Instant test data collection: To provide rapid assistance when troubleshooting, a customer administrator can initiate a test immediately. This test will run straight away without waiting for a scheduled event. The data collected is identical to a scheduled test.

[Remainder of this page intentionally left blank]

Personal Data Processing

The tables below list the personal data used by ThousandEyes to carry out the services and describes why ThousandEyes processes the data.

Personal Data Processed by ThousandEyes, Generally	Purpose of Processing
<u>Administrative Information:</u> <ul style="list-style-type: none"> User email address User first and last name User Password User IP address Billing contact name 	<ul style="list-style-type: none"> Activation of service Billing/invoicing Product notifications Technical support Authentication/Authorization Activity logs
<u>Performance metrics:</u> <ul style="list-style-type: none"> IP address and logged-in username for the end user computer where endpoint agent is installed 	<ul style="list-style-type: none"> Measure network performance against either internal or public internet-based network assets

Additional Personal Data Customer Can Configure to be Processed by the ThousandEyes Endpoint Agent	Purpose of Processing
Usage information the customer's administrator configures the platform to collect could include: <ul style="list-style-type: none"> Name of the logged-in user account or endpoint identifier Administrator-selected website page names, object names on target pages (for load time monitoring) Computer hostname 	<ul style="list-style-type: none"> Measure network performance against either internal or public internet-based network assets

[Remainder of this page intentionally left blank]

Personal Data Processed for Technical Assistance and Support	Purpose of Processing
Support Information: <ul style="list-style-type: none"> • First name, Last name, Email, Phone number of the individual opening the service request • Customer account information 	<ul style="list-style-type: none"> • Technical support • Review of the support service quality • Troubleshooting • Analysis of service

Cross-Border Transfers

Except as it relates to the provision of technical support, as set forth below, ThousandEyes only processes Personal Data in the United States. ThousandEyes utilizes a 24/7 “follow the sun” technical support model, leveraging support engineers in Australia, Bulgaria, Ireland, Singapore, Slovenia, USA, and the United Kingdom. ThousandEyes may update this list of countries from time to time in its sole discretion. To subscribe to receive updates, please follow the instructions in the first paragraph of this document.

Personal Data Access Control

The tables below list the personal data used by ThousandEyes to carry out the services and describes who accesses the data.

Personal Data Processed by ThousandEyes	Who Has Access	Purpose of the Access
Registration and Administrative Information	<ul style="list-style-type: none"> • Customer Administrator • ThousandEyes 	<ul style="list-style-type: none"> • Modify and control certain administrative information • Provision customer’s account; billing/invoicing; supporting the service in accordance with ThousandEyes’s data access and security controls process
Usage Information	<ul style="list-style-type: none"> • Customer Administrator • ThousandEyes 	<ul style="list-style-type: none"> • Measure network performance against either internal or public internet-based network assets

[Remainder of this page intentionally left blank]

Personal Data Access Control

The table below lists Personal Data retention periods for different features of the ThousandEyes platform.

Type of Data	Retention Period	Criteria for the Retention
Usage Information, Raw DNS query data (domain, DNS record type, DNS response, IP address) and Device ID	90 days	Automatically deleted after 90 days
Administrator email address, activation code, Administrator first and last name, password, Company name, billing contact name	Data is deleted upon request	n/a

Deletion

A customer may request deletion of Personal Data by emailing privacy@thousandeyes.com. When customer makes a request for deletion, ThousandEyes will purge the Personal Data from its systems, except for administrative data required for legitimate business purposes (e.g. billing records, audit logs, taxes).

Third Party Service Providers (Sub-processors)

A current list of ThousandEyes's third party service providers having access to Personal Data is available at <https://thousandeyes.com/subprocessors>. If you would like to receive notifications when this list is updated, please email privacy@thousandeyes.com.

Data Protection and GDPR FAQ

WHAT DOES THOUSANDEYES'S SECURITY AND PRIVACY PROTOCOL ENTAIL?

ThousandEyes takes a systematic approach to data protection, privacy, and security. We believe a comprehensive security and privacy program requires executive sponsorship and active involvement of cross-functional stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization.

ThousandEyes has established formal policies and supporting procedures concerning the privacy, security, review, and management of our products and services. The ThousandEyes Chief Information Security Officer maintains overall responsibility for the program which is evaluated on a regular basis by a Information Security Steering Committee, and an independent third party performs an annual AT Section 101 attestation that produces a SOC2 Type II report. Also, the Information Security Management System supporting our network performance management software as a service application received the ISO/IEC 27001:2013 certificate from an independent certification body. Additionally, to demonstrate transparency of its security controls, ThousandEyes participates in the Cloud Security Alliance (CSA) Consensus Assessments Working Group, and our assessment can be obtained online.

ThousandEyes has been awarded TrustArc's TRUSTe Privacy Seal signifying that our privacy policy and practices have been reviewed by TRUSTe for compliance with (i) TRUSTe's Program Requirements, (ii) the TRUSTed Cloud Program Requirements, and (iii) the EU/Swiss-U.S. Privacy Shield, including transparency, accountability and choice regarding the collection and use of personal information.

For additional information, please visit: <https://app.thousandeyes.com/privacy>

HOW DOES THOUSANDEYES COMPLY WITH EUROPEAN DATA PROTECTION LAWS?

In addition to implementing a comprehensive privacy and data security program, ThousandEyes complies with applicable privacy laws and endeavors to follow best practices set out in relevant guidance. This regards the protection of individuals when processing personal data and the free movement of data (the “Privacy Directive”), as implemented into local laws, Switzerland’s Federal Act on Data Protection of June 19, 1992, Germany’s Federal Data Protection Act of December 20, 1990 as amended on September 14, 1994, and the GDPR.

WHAT IS GDPR AND WHO DOES IT AFFECT?

The European Union General Data Protection Regulation, or GDPR, became law on May 25, 2018, and affects organizations that process EU personal data. Aimed at protecting the fundamental right to privacy, the new regulations are broad, strict, and require adherence from organizations all over the world.

WHAT IS THOUSANDEYES’S STANCE ON DATA PRIVACY IN GENERAL?

Since inception, protecting the security and privacy of our customers’ data has been a top priority for ThousandEyes. Our customers trust us to collect and store information about performance of networks and applications they use. Depending on the deployment scenario and specific customer use cases, this could include information from the Internet that constitutes public domain knowledge and/or information from private enterprise networks. As such, we treat all data collected as confidential and have implemented a security program designed to ensure its confidentiality, integrity, availability, and privacy.

We start with a solid management foundation through adoption of the widely recognized and respected ISO/IEC 27001 standard for our information security management system. Our privacy management system is based on the Privacy Shield Framework, which was developed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

Jointly these form a ThousandEyes Unified Security and Privacy Management Framework (USPMF) that is supported by strict policies, standards, technologies and processes. We continually improve our USPMF by implementing additional technical and organizational controls to ensure customer data is always protected with best current practices.

To learn more, please visit: www.thousandeyes.com/trust