Trellix **Privacy Data Sheet** We bring security to life.

Trellix ePolicy Orchestrator on Premises (ePO - On-prem)

The purpose of this Privacy Data Sheet is to provide customers of Trellix ePO - On-prem with details on how Trellix captures, processes, and stores[1] telemetry information, including personal data (or personally identifiable information), to help them understand and assess the impact of the telemetry capabilities on their overall privacy posture.

Trellix ePO - On-prem is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malware, suspicious communications, and unsafe websites and files, and is made available by Trellix to companies or persons who obtain a Trellix ePO - On-prem subscription.

Trellix will process personal data from ePO - On-prem in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Trellix is the Data Controller for the personal data processed to administer and manage the customer relationship. Trellix is the Data Processor for the personal data processed by the ePO - On-prem service to provide its functionality.

This Privacy Data Sheet is a supplement to the Trellix Website Privacy Notice.

Product Overview

The Trellix ePO - On-prem platform enables centralized policy management and enforcement for Customers’ endpoints and enterprise security products. Trellix ePO - On-prem monitors and manages the Customer’s network, collects data on events and alerts, creates reports, and automates workflow to streamline product deployments, patch installations, and security updates. As an open and comprehensive platform, ePO - On-prem integrates more than 150 third-party solutions for faster and more accurate responses.

[1] In this document, we adopt the broad definition of “processing” that appears at Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …”, which includes, but is not limited to the following non-exhaustive series of examples: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Trellix ePO - On-prem serves as the command center for data security and management across the Customer’s entire enterprise by introducing an integrated single pane view for automated and proactive policy management and enforcement.

Customers use the Trellix ePO - On-prem console to gain critical visibility of enterprise security across all vectors—file, web, message, and network, and to enable action across the full spectrum of new and emerging threats in real-time, from anywhere.

As the organization's command center, Customers use ePO - On-prem to access managed clients, networks, data, and compliance solutions to protect their networks.

Trellix ePO - On-prem's system infrastructure is located within the Customer’s environment and can be managed 24/7 by a team of Trellix security experts. ePO - On-prem removes the setup and maintenance of security infrastructure, allowing the Customer to focus exclusively on monitoring and proactively addressing emerging threats on all enterprise devices.

Trellix ePO - On-prem solution manages data generated by other Trellix products and services, including:

- Trellix Endpoint Security (ENS) (Includes Adaptive Threat Protection (ATP))
- Trellix Endpoint (for Windows 10 only)
- Trellix Insights
- Data Loss Prevention (DLP)
- Threat Intelligence Exchange (TIE)
- Trellix Management of Native Encryption (MNE)
- Skyhigh Client Proxy (SCP)

Trellix ePO - On-prem works in tandem with other Trellix security products and/or services to stop malware attacks and to notify Customers when an attack occurs. Proactive device security is deployed across the entire enterprise, eliminating manual efforts to install or update security for each device which assures stronger enforcement against malware, including known and unknown threats. For a managed deployment of ePO - On-prem, updates to the platform are automatic, continuous and transparent.

Products and/or services within the Customer’s environment that integrate with ePO - On-prem may use the Registered Server feature for threat event generation and policy management, then leverage the Trellix Agent to send security and product and/or system information to the database/server designated by the Customer.

The Trellix ePO - On-prem solution allows Customers to perform network and client tasks, including:

- Managing and enforcing network and endpoint security using policy assignments and client tasks;
- Monitoring the health of the Customer’s network;
- Capturing data on events and alerts;
- Creating reports using the query system builder, which displays configurable charts and tables of the Customer's network security data;
- Automating product deployments, patch installations, and security updates.

With ePO - On-prem, the Customer's ePO - On-prem Administrator (ePO Admin) can:

- Grant user access to specific groups of systems or give administrators full control;
- Install an open framework that unifies security management for systems, applications, networks, data, and compliance solutions;
- Unify security management across endpoints, networks, data, and compliance solutions from Trellix and third-party solutions;
- Define how Trellix ePO - On-prem software directs alerts and security responses based on the type and criticality of security events in the Customer's environment.

Trellix ePO - On-prem can be implemented as one of two deployments:

- **Standalone implementation:** In standalone deployments, the ePO - On-prem solution reads data stored on the Customer's enterprise systems and no data is ever captured by Trellix.
- **Managed implementation:** In managed ePO - On-prem deployments, Customers use tenant credentials (Trellix Agent) for ePO - On-prem to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities, and status of their systems within their organization.

The ePO - On-prem solution also enables Customers to easily migrate to Trellix ePO - SaaS and take full advantage of the many efficacies and benefits of the SaaS-based security management platform.

Personal Data Processing

The ePO - On-prem solution works in tandem with other Trellix security products and/or services and offers the Customer's ePO Admin the ability to set enterprise policies and configurations for the Customer's enterprise endpoint systems.

Trellix Agent enables communication between the Customer's enterprise endpoints and the ePO - On-prem service by way of Web API, which allows access to data via scripting. ePO - On-prem then processes and stores data generated by Customer enterprise endpoints located within the Customer's environment.

Trellix ePO Admins require independent logins for authentication. At the sole discretion of the ePO Admin, the registered ePO - On-prem server/database can capture data from the Customer's enterprise endpoint system in an authorized on-premises Active Directory through the Registered Server feature. This functionality is commonly used to reduce management tasks required of the ePO - On-prem Admin, such as managing the System Tree or managing product policies by user group.

The event data and system properties can contain elements of personal data relevant to endpoint security. For example, if a threat is detected on an endpoint, the threat event may contain the IP address of the system, and/or the logged-on username. In addition, system properties may contain personal data such as machine names, agent GUIDs, and IP addresses.

As a result, the ePO - On-prem service may process a range of data potentially containing personal information. The table below shows the personal data processed by ePO - On-prem to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix ePolicy Orchestrator On-Premises

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● User ID ● Trellix Agent GUID, ● First Name and Last Name ● Email address of ePO Admin ● Registered Server Credentials (if using Registered Servers feature) ● Company billing address ● Active Directory username (optional configuration through if enabled by ePO Admin) ● Tenant ID (GUID) ● Company billing address ● Machine name ● Mac address ● IP address ● Timestamps ● AD Username (if enabled)	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.
Generated Data	Incidents / Events: ● Threat details ○ Location ○ Action Taken ○ URL ○ URL with search strings Evidence: ● File ● File Name ● File Location	Used for threat detection, system communication and management.
Collected Data	Configuration Information: ● Product versions/extensions installed ● ePO server version ● License key ● Node-count managed	Used to integrate with user management and evidence storage systems.

*** Please note the Personal Data Categories explained below and used throughout Privacy Data Sheets for Trellix products and/or services:**

- **Administrative Data**: Information to enable the service and/or manage the customer relationship;

- **Generated Data**: Information generated by the product (events, evidence, logs);
- **Collected Data:** Information generated by the Customer (policies and configurations).

Data Center Locations

For standalone implementation, the data center is located within the Customer's environment.

For managed ePO - On-prem implementation, Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. ePO - On-prem processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Germany, Australia, Singapore, and India. Trellix's regional clouds provide options to address customers' data location preference. Customers have the choice to select a region or to default to their nearest region for data processing. This means that, unless otherwise modified by a system administrator, the traffic in certain countries will be directed to a defined compute location.

Table 2. Data Center Locations

Data Center Provider	Data Center Location
AWS	AWS West (Oregon)
AWS	Germany (Frankfurt)
AWS	Australia (Sydney)
AWS	Singapore
AWS	India (Mumbai)

Subprocessors

Trellix partners with service providers that act as subprocessors for the ePO - On-prem service and contract to provide the same level of data protection and information security that Customers can expect from Trellix. A current list of subprocessors for the service is below:

Table 3. Subprocessors

Subprocessor	Personal Data Category	Service Type	Location of Data Center
AWS	See Table 1	Data Center	AWS West (Oregon)
AWS	See Table 1	Data Center	Germany (Frankfurt)
AWS	See Table 1	Data Center	Singapore
AWS	See Table 1	Data Center	India (Mumbai)
OKTA	See Table 1	Authentication	AWS West (Oregon)

Cross-Border Data Transfer

In the event of a need to share personal information with Trellix personnel in regions outside of those identified in the Data Center Locations section above, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission and/or other legal instruments recognized by EU data protection laws. For a more detailed assessment of our international data transfers, please refer to the Trellix Transfer Impact Assessment statement.

Access Control

Access to customer information is subject to Trellix's Access Management Policy. Access is protected by multiple authentication and authorization mechanisms. Trellix has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based on roles and job functions. Shared accounts are prohibited. All usernames are traceable to a specific human user. User access credentials are promptly removed when user access is no longer authorized (e.g., Trellix employment terminates).

Remote user access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA are required.

The table below lists the personal data used by ePO - On-prem to carry out the service, who can access that data, and why.

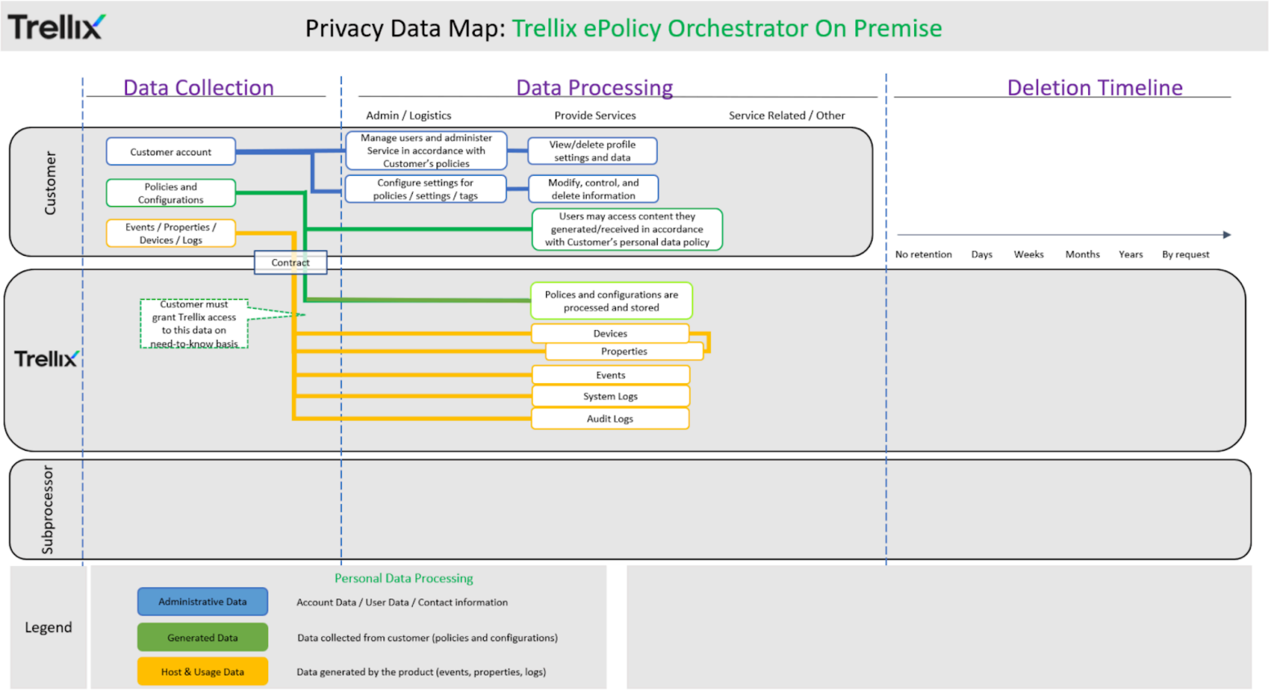
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Analysis of User/Systems suspected of malware detection/detonation and cleanup or quarantine of the same. Also, to provide data on suspected violations of policy, compliance, and reporting.
	Trellix	Debugging of Customer/operational data in the event of an escalation.
Generated Data (Incidents / Events)	Customer	Analysis of User/Systems involved in violations, compliance, and reporting.
	Trellix	Debugging of Customer/operational data in the event of an escalation.
Generated Data (Evidence)	Customer	Associate evidence of a reported violation.

	Trellix	No access.
Collected Data	Customer	Leverage user groups in AD to define end-user permissions. S3 provides customer-controlled storage for evidence.
	Trellix	Give functionality to apply polices.

Trellix ePolicy Orchestrator on Premise (ePO - On-prem) Data Flow Diagram

The key data flows associated with the information processing activities described in this document are shown below.


Trellix
Privacy Data Map: Trellix ePolicy Orchestrator On Premise
Data Collection
Data Processing
Deletion Timeline
Admin / Logistics
Provide Services
Service Related / Other
Customer
Customer account
Policies and Configurations
Events / Properties / Devices / Logs
Manage users and administer Service in accordance with Customer's policies
Configure settings for policies / settings / tags
View/delete profile settings and data
Modify, control, and delete information
Users may access content they generated/received in accordance with Customer's personal data policy
Contract
No retention
Days
Weeks
Months
Years
By request
Trellix
Customer must grant Trellix access to this data on need-to-know basis
Polices and configurations are processed and stored
Devices
Properties
Events
System Logs
Audit Logs
Subprocessor
Legend
Personal Data Processing
Administrative Data
Account Data / User Data / Contact information
Generated Data
Data collected from customer (policies and configurations)
Host & Usage Data
Data generated by the product (events, properties, logs)

Customer Privacy Options

Trellix designs its products to support our customers' compliance with global data protection and compliance obligations. It does this by addressing threat intelligence and security challenges at the application, network, and endpoint levels, and in the cloud. In addition, Trellix offers product features that help our customers meet their EU General Data Protection Regulation (GDPR) and other legal compliance goals. Such features include, but are not limited to data localization options, policy enforcement, access controls, logging capabilities, individual rights processing, and cross-border data transfer mechanisms.

Customers control whether the Trellix ePO - On-prem’s service is enabled or disabled. When it is disabled, no data processed by the service is collected and sent to the cloud and no data is downloaded by ePO - On-prem from the cloud data centers.

Data Portability

Except with respect to Registration Information, the Customer can forward personal data processed by ePO - On-prem to a third-party data store. If applicable, to effectuate data portability, Customers may request assistance from Trellix Engineering for a large-scale movement of data (e.g., if the Customer does not renew subscription and asks for all data to be transferred to a third-party data store).

Data Deletion and Retention

The table below lists the personal data used by ePO - On-prem, the length of time that data needs to be retained, and why we retain it, if applicable. For ePO - On-prem, the Customer (rather than Trellix) determines applicable retention periods, based on the Customer’s own policies.

A data subject may request deletion of his or her Personal Data by sending a data subject request as described below in this Privacy Data Sheet.

A customer may request data deletion by submitting a ticket to Trellix support at support_reply@trellix.com. When a customer makes a request for deletion, Trellix will purge the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records).

Table 5. Data Retention

Personal Data Category	Retention Period	Reason for Retention
Administrative Data	Retained until Customer deletes it.	Compliance, reporting, troubleshooting.
Generated Data	Not Applicable.	Not Applicable.
Collected Data	Not Applicable.	Not Applicable.

Personal Data Security

Files stored on or processed by Trellix’s systems are secured with state-of-the-art technologies, and Trellix implements rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Table 6. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Administrative Data	See Table 1	Encrypted in transit and at rest
Generated Data	See Table 1	Encrypted in transit and at rest
Collected Data	See Table 1	Encrypted in transit and at rest

Additional details for product certification are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in global and regional clouds. We will not access the content of files in a way in which we could learn meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats.

The Trellix Privacy Office and Trellix Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Trellix products and services. ePO - On-prem is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Trellix also maintains third-party validations to demonstrate our commitment to information security.

Exercising Data Subject Rights

Users whose personal data is processed by ePO - On-prem may have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the service.

We will confirm identification (typically with the email address associated with a Trellix account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Where Trellix is a Data Processor, users may be redirected to the Data Controller (e.g., the user’s employer) or other organization for an appropriate response.

Requests can be made by submitting a request via:

1) the Trellix Individual Data Request Form

2) by postal mail:

In the U.S. by registered mail:
Musarubra US LLC
Attn: Legal Department –Privacy
6000 Headquarters Drive, Suite 600

Plano, Texas, 75024

or call us at +1 (214) 494-9190

In the European Economic Area by registered post:
Musarubra Ireland Limited
Attn: Legal Department –Privacy
Building 2000, City Gate

Mahon, Cork, Ireland

or call us at +353 21 467 2000

In Japan by registered mail:
Musarubra Japan KK
Attn: Legal Department –Privacy
Shibuya Mark City West

1-12-1 Dogenzaka, Chibuyaku, Tokyo 150-0043

About This Data Sheet

Trellix Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis.

The information provided in this document is for general awareness only, may be subject to change, and does not constitute legal or professional advice. Except as provided by the terms of a written agreement, the information and services described herein are provided "as is" with no warranty of any kind.