Trellix Privacy Data Sheet We bring security to life.

# Trellix Insights

The purpose of this Privacy Data Sheet is to provide Customers of Trellix Insights 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 Insights is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malware, suspicious communications, unsafe websites and files made available by Trellix to companies or persons who obtain a Trellix Insights subscription.

Trellix will process personal data from Insights 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 Trellix Insights in order to provide its functionality.

Note: This Privacy Datasheet is a supplement to the Trellix Website Privacy Notice.

## Product Overview

Trellix Insights proactively monitors and prioritizes local and global threats and campaigns predicted to affect Customers' enterprise endpoint environment. With the help of machine learning analysis, Customers use Trellix Insights to determine a comprehensive security posture based on distributed enterprise endpoints and an open integration with Trellix intelligence clouds. Trellix Insights then takes preemptive measures to immediately and proactively address known and unknown cyber-threats and efficiently prevents and/or mitigates cyber-attacks. Trellix Insights then prescribes to Customers the steps needed to optimize the security stance.

[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."

Insights capabilities preemptively improve defensive countermeasures and accelerates response times while utilizing fewer resources. Trellix Insights minimizes the need for human actors to reactively and imprecisely respond to cyber-threats and optimizes remediation resources to mitigate any known or unknown cyber-attack.

Risk intelligence gathered and refined from one billion sensors distributed across global threat intelligence resources and assessed by proven advanced threat researchers empowers Trellix Customers to prioritize its security and cyber defenses.

Detection, remediation, accelerated preemptive response times, and significant risk reduction can be realized from one console utilizing Trellix Insights. Intelligence and actionable insights from the Trellix Insights console give Customers' SecOps Admins the best possible cybersecurity stance against known and unknown cyberthreats, and boosts confidence in the entire enterprise's cyber defenses. Customers use Trellix Insights to assimilate critical threat information quickly (from weeks down to seconds).

Combined with other Trellix offerings (including, for example, Trellix ePolicy Orchestrator (Trellix ePO) and Trellix Endpoint Security (Trellix ENS)), the Trellix Insights solution leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time, across all vectors—file, web, message, and network.

**Trellix Insights can be implemented as one of two deployments:**

- ✓ **Trellix Insights via ePolicy Orchestrator on Premise (ePO On - Prem) managed deployment**:

  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 managed endpoint systems within their organization;

- ✓ **Trellix Insights via ePolicy Orchestrator SaaS (ePO - SaaS) managed deployment**: Customers use tenant credentials (Trellix Agent) for ePO - SaaS to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities, and status of their managed Windows systems within their organization.

Please see Trellix Insights for additional information related to the Trellix Insights solution. Please also see Trellix ePolicy Orchestrator on Premise (ePO On-Prem) and the Trellix ePolicy Orchestrator SaaS (ePO-SaaS) Privacy Data Sheets for additional information.

## Personal Data Processing

Trellix Insights uses Trellix machine learning technology and human intervention to proactively and automatically monitor and detect malicious activity and policy violations. Trellix's machine learning modules analyze event information, in online and offline modes, from the Customer's enterprise endpoint environment.

Trellix Insights will capture information from the Customer's Trellix ePolicy Orchestrator (ePO) service which includes telemetry data distributed across the Customers' network infrastructure. Because of this, Trellix Insights will capture information differently depending on the deployment version.

- **Trellix ePolicy Orchestrator on Premise (ePO On - Prem) managed deployment:** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - Prem) server/database present within the Customer's network environment.
- **Trellix ePolicy Orchestrator SaaS (ePO - SaaS) managed deployment:** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix's instance in Amazon Web Services (AWS) regional clouds.

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

**Table 1. Personal Data Processed by Trellix Insights**

| Personal Data Category | Types of Personal Data Processed | Purpose of Processing |
|---|---|---|
| Administrative Data | ● ePO ID<br>● Tenant ID<br>● Trellix Agent ID (Pseudonymized data) | Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting. |
| Generated Data | Endpoint telemetry from several products and scanner technologies and each scanner provides the following details<br>Incidents / Events:<br>● Threat details<br>○ Location<br>○ Action Taken<br>○ URL<br>○ URL with search strings<br>Evidence:<br>● File<br>● File Name<br>● File Location | Endpoint management, compliance, auditing, and threat analysis. |
| Collected Data | ● ePO ID<br>● Tenant ID<br>● Trellix Agent ID (Pseudonymized data) | Used to Integrate with Customer management systems. |

***The Personal Data Categories used in this, and other Trellix Privacy Data Sheets are:**

**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 ePolicy Orchestrator On-Prem deployment,** the data center is located within the Customer's network infrastructure.

**For ePolicy Orchestrator SaaS managed deployment,** Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Insights processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) data centers regional clouds located in the United States, Australia, Germany, and Singapore. Trellix's regional clouds provide options to address Customers' data location preferences. 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 | Australia (Sydney) |
| AWS | Germany (Frankfurt) |
| AWS | Singapore |
| AWS | AWS East (Virginia) |
| AWS | India (Mumbai) |

## Subprocessors

Trellix partners with service providers that act as subprocessors for the Insights service and contracts to provide the same level of data protection and information security that you 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 | Hosting | AWS West (Oregon) |
| AWS | See Table 1 | Hosting | Australia (Sydney) |
| AWS | See Table 1 | Hosting | Germany (Frankfurt) |
| AWS | See Table 1 | Hosting | Singapore |
| AWS | See Table 1 | Hosting | AWS East (Virginia) |
| AWS | See Table 1 | Hosting | 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 Insights to carry out the service, who can access that data, and why.

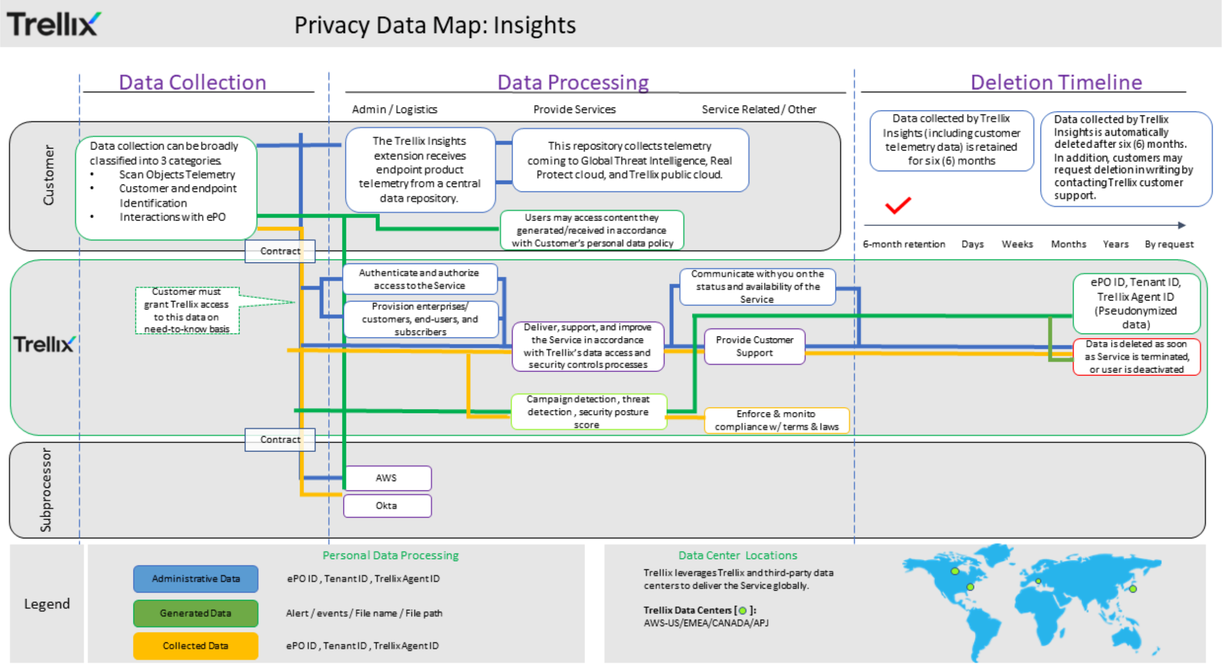
**Table 4. Access Control**

| 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 | Customer | Analysis of User/Systems involved in violations, compliance, and reporting. |
| | Trellix | Debugging of Customer/operational data in the event of an escalation. |
| Collected Data | Customer | Associate evidence of a reported violation. |

| | | |
|---|---|---|
| | Trellix | Debugging of Customer/operational data in the event of an escalation. |

## Trellix Insights Data Flow Diagram

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



Data collection can be broadly classified into 3 categories.
- Scan Objects Telemetry
- Customer and endpoint Identification
- Interactions with ePO

The Trellix Insights extension receives endpoint product telemetry from a central data repository.

This repository collects telemetry coming to Global Threat Intelligence, Real Protect cloud, and Trellix public cloud.

Users may access content they generated/received in accordance with Customer's personal data policy

Customer must grant Trellix access to this data on need-to-know basis

Authenticate and authorize access to the Service

Provision enterprises/ customers, end-users, and subscribers

Deliver, support, and improve the Service in accordance with Trellix's data access and security controls processes

Communicate with you on the status and availability of the Service

Provide Customer Support

Campaign detection , threat detection , security posture score

Enforce & monito compliance w/ terms & laws

Data collected by Trellix Insights (including customer telemetry data) is retained for six (6) months

Data collected by Trellix Insights is automatically deleted after six (6) months. In addition, customers may request deletion in writing by contacting Trellix customer support.

ePO ID, Tenant ID, Trellix Agent ID (Pseudonymized data)

Data is deleted as soon as Service is terminated, or user is deactivated

| | |
|---|---|
| Administrative Data | ePO ID , Tenant ID , Trellix Agent ID |
| Generated Data | Alert / events / File name / File path |
| Collected Data | ePO ID , Tenant ID , Trellix Agent ID |

Trellix leverages Trellix and third-party data centers to deliver the Service globally.

**Trellix Data Centers [ ● ]:**
AWS-US/EMEA/CANADA/APJ

## 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 Insights 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 the service from the cloud data centers.

## Data Portability

Except with respect to Registration Information, the Customer has the ability to forward the personal data processed by Trellix Insights to a third-party data store. Customers may request assistance from Trellix Engineering for a large-scale movement of data (e.g., 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 Trellix Insights, the length of time that data needs to be retained and why we retain it.

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; user accounts in SaaS enterprise products are usually not auto deleted even when their subscription has ended. | Duration of subscription contract. |
| Generated Data | 6 months. | Duration of subscription contract & retrospective detection capabilities in the product. |
| Collected Data | Retained until the Customer deletes or until the subscription service ends. | Duration of subscription contract. |

## Personal Data Security

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

Insights uses a secure portal hosted by AWS to store engagement data. Data collection is accomplished by downloading an executable tool to the Customer's environment where queries and API calls are performed against Trellix products. The collected data is then encrypted using 256-bit encryption as an output file and uploaded via secure SSL connection to the AWS Trellix server where it is processed and stored in the encrypted database.

AWS audits and certifies their environment on a regular basis by a third-party vendor. AWS is compliant with dozens of standards including NIST, ISO, SOC, CSA, PCI, GDPR, etc. The latest audit reports are available on the AWS website and can be found once logged into the AWS Console.

For additional details on AWS certifications, visit https://aws.amazon.com/.

- Search for “Artifact”
- Select Artifact from the search results
- Select View Reports from the AWS Artifact page

**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 certifications are available upon request.

## Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional Insights 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 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. The Service 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 the Service 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. Please note, users whose employer is the Customer/Controller may be redirected to their employer for a 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.

Please note that the information provided with this document concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.