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

Trellix Data Loss Prevention (DLP)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix DLP with details on how Trellix DLP Products and Services capture, process, and store[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 DLP is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malwares, suspicious communications, unsafe websites and files, and is made available by Trellix to companies or persons who obtain a Trellix DLP subscription.

Trellix will process personal data from DLP 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 DLP service to provide its functionality.

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

Product Overview

The Data Loss Prevention solution suite includes:

Trellix DLP Endpoint provides comprehensive protection for all potential leaking channels, including removable storage devices, the cloud, email, instant messaging, web, printing, clipboard, screenshot, and file-sharing applications, and is provided to companies or persons who obtain a Trellix DLP subscription.

Trellix DLP Discover helps organizations identify and manage risk of data loss by locating, inventorying, classifying, and protecting corporate data on both the premises and in the cloud. DLP Discover protects data file shares, databases and Box repositories.

[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 DLP Prevent and/or Monitor helps organizations identify and manage risk of data loss in the network by inspecting network traffic for DLP violations using policies configured by customers. DLP Prevent enforces policies using SMTP or ICAP Protocols and can block network uploads. DLP Monitor can inspect and notify network data in real time.

Please see Trellix Data Loss Prevention for additional information related to the Trellix Data Loss Prevention solution.

Personal Data Processing

Data definitions (registered documents, EDM data, regex, dictionaries), configurations, policies, rules, incidents, and evidence files may contain personal data which are processed and stored in third-party storage locations. Configurations, rules, incidents, and policies are processed and stored in Trellix's instance in Amazon Web Services, Inc. (AWS) data centers. DLP always runs behind the customer's premises. However, when DLP is configured by the applied policy, it uploads encrypted events to Trellix's instance in AWS datacenters and encrypts evidence files to a Customer managed AWS S3 bucket.

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

Table 1. Personal Data Processed by Trellix Data Loss Prevention

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● Username ● Email address ● IP address ● MAC address ● Host name ● Device serial number ● Domain name ● Operating system ● CPU information ● Memory usage ● Disk usage ● Time zone ● Last time booted ● Last communication time	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.

Generated Data	Incidents/Events: ● File name ● Application ● URL ● Uploaded text ● Clipboard text Evidence: ● File contents	Endpoint management, compliance, auditing, and threat analysis.
Collected Data	Configuration information: ● Active Directory group ● AWS S3 bucket name	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: Generated information may include personal data processed about malware, threats, actual or attempted security events, including but not limited to their frequency, source, associated code, general identifiers, attacked sectors and geographies;

Collected Data: Configuration information derived from the Customer environment.

Please also note, the "Customer employees" Personal Data Category includes data collected off an endpoint during normal operations. The "Customer administrator" Personal Data Category includes data entered in the Trellix ePolicy Orchestrator (ePO) server/database which could be transmitted to an endpoint to facilitate integrations.

Data Center Locations

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. DLP processes the personal data in Trellix's instance in AWS (Amazon Web Services) regional clouds located in the United States and/or Germany. 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)

Subprocessors

Trellix partners with service providers that act as subprocessors for the DLP service and contract 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	Germany (Frankfurt)

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 by 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 Trellix DLP to carry out the service, who can access that data, and why.

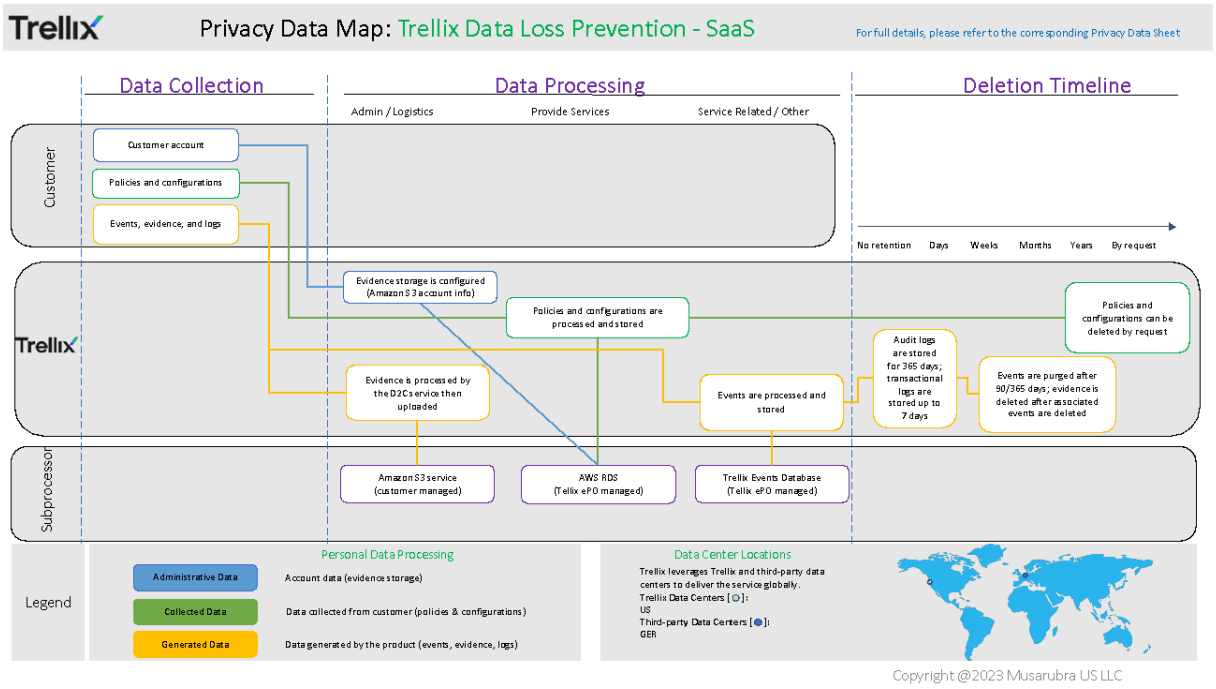
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	**Customer** SaaS ePO provides the capability of user access control to limit access to the data.	Analysis of user / systems involved in violations, compliance and reporting

	The admin tenant of the Customer can use role-based access to grant selective access.	
	Trellix Access is available to DevOps and senior engineering architects controlled through MFA.	Debugging of the Customer data in the event of an escalation.
Generated Data (Incidents/Events)	**Customer** SaaS ePO provides the capability of user access control to limit access to the data. The admin tenant of the Customer can use role-based access to grant selective access.	Analysis of user / systems involved in violations, compliance and reporting.
	Trellix Access is available to DevOps and senior engineering architects controlled through MFA.	Debugging of Customer data in the event of an escalation.
Generated Data (Evidence)	**Customer** Stores evidence files on S3 buckets owned by their AWS account. Customer is responsible to safeguard access to evidence file using access privileges provided by AWS.	Associate evidence to a violation reported by DLP.
	Trellix No access to evidence file on customer's S3 bucket	No access.
Collected Data	**Customer** Owner of Active Directory (AD) and S3 bucket. Configures them on SaaS ePO for DLP to use.	Leverage user groups in AD to define end-user permissions in DLP policies. S3 provides customer-controlled storage for evidence.
	Trellix Read AD to get user information which is appended on the events data. Send evidence files to S3 bucket.	Give functionality to apply polices based on AD.

Trellix Data Loss Prevention (DLP) Data Flow Diagram

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



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, 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 DLP 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 DLP from the cloud data centers.

Data Portability

Except with respect to Registration Information, the Customer can forward the personal data processed by Trellix DLP 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., 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 DLP, 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 the Customer removes associated endpoint	Compliance, reporting, troubleshooting
Generated Data (Incidents/Events)	90 days or 365 days depending on the SKU purchased	Compliance, reporting
Generated Data (Evidence)	90 days after all linked incidents/events are purged	Compliance, reporting
Collected Data	Retained until the Customer deletes	System integrations

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.

DLP uses a secure portal hosted by AWS to store Customer information. 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 http: //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 certification are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the 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 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.