Trellix Privacy Data Sheet We bring security to life.

Trellix Drive Encryption

The purpose of this Privacy Data Sheet is to provide Customers of Trellix Drive Encryption 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 Drive Encryption is an enterprise-grade full disk encryption solution that encrypts server, desktop, laptop and tablet storage devices, enforcing strict access control to prevent unauthorized access to the underlying data.

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

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

Product Overview

Trellix Drive Encryption features deliver encryption that protects data from unauthorized access, loss, and exposure using preboot authentication and a powerful encryption engine. The Drive Encryption suite provides multiple layers of defense against data loss with integrated modules that address specific areas of risk. Drive Encryption provides protection for individual computers and roaming laptops with Basic Input Output System (BIOS) and Unified Extensible Firmware Interface (UEFI).

The Drive Encryption solutions allows Trellix Customers to:

- Enforce access control settings using pre-boot authentication;
- Apply certified encryption algorithms (FIPS, Common Criteria);

[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."

- Support mixed-device environments, including solid-state drives;
- Support Trusted Computing Group (TCG) Opal v1.0 self-encrypting drives.

The Drive Encryption solution includes encryption software installed within Trellix Customers' network environment and integrates with Trellix's ePolicy Orchestrator's On-Premises (ePO On-Prem) command center interface and captures information through the ePO server. Applied Customer security policies are utilized through the Drive Encryption solution which are enforced throughout the Customer's entire network infrastructure. Drive Encryption's disk encryption process is transparent to the Security Operations Administrators (SecOps Admins) and Security Operators (Sec Ops) team members and has minimal impact on CPU or overall device performance.

Trellix Drive Encryption delivers powerful encryption solutions that protect against unauthorized access of data, data loss, and unintended exposure of important data. Trellix Drive Encryption encrypts all computer disk drives integrated within Trellix Customers' network infrastructure and secures the data within a device, where data is stored at rest. Only authorized users who are authenticated in a pre-boot environment will have capabilities to access the data locally stored on the device.

Devices within the Customer network infrastructure running Trellix Drive Encryption are managed from ePO's command center. Drive Encryption integrates with ePO services located entirely within the Customer's network infrastructure or integrated with Trellix's instance in Amazon Web Services (AWS).

Data Protection Self Service Portal (DPSSP) is an optional companion to the Drive Encryption solution. DPSSP is an extension that integrates with ePO On-Premises services to allow SecOps Admins to configure a web portal user interface for end users to retrieve recovery keys to unlock the device where log on has failed, without the need to contact an IT support team directly to remediate the issue.

Trellix Drive Encryption features provide full disk encryption for Microsoft Windows laptops and desktop PCs and prevents the loss of sensitive data, especially from lost or stolen equipment.

Trellix Drive Encryption includes the following security features:

- **Centralized management** — Drive Encryption integrates fully into Trellix ePO - On-Prem, leveraging the Trellix ePolicy Orchestrator infrastructure for automated security reporting, monitoring, deployment, and policy administration.
- **Transparent encryption** — Drive Encryption enables transparent encryption without hindering users or system performance.
- **Access control** — Drive Encryption enforces access control with Pre-Boot Authentication (PBA).
- **Recovery** —The recovery feature allows the user to perform emergency recovery when the system fails to reboot, or its Pre-Boot File System (PBFS) is corrupt.
- **Support for self-encrypting drives** — Drive Encryption and Trellix ePO - On-prem enable centralized management of self-encrypting drives that conform to the Opal standard from Trusted Computing Group (TCG), including locking and unlocking, reporting, recovery, policy enforcement, and user management.
- **Trusted Platform Module (TPM)** — Drive Encryption supports TPM 2.0 on Windows 8 and later UEFI systems to provide platform authentication without the need for PBA.

Trellix Drive Encryption can be implemented as a managed deployment:

✓ **Trellix Drive Encryption via ePolicy Orchestrator on Premise (ePO On - Prem) 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 network environment within their organization;

- Note that Customers can use the Offline Activation feature to activate Drive Encryption within a Customer's network infrastructure without connecting to the Trellix ePO On-Prem server.

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

Please also see Trellix ePolicy Orchestrator on Premises (ePO On-Prem) for additional information related to the ePolicy Orchestrator solution.

Personal Data Processing

Trellix Drive Encryption encrypts Trellix Customers' computer disk drives across their entire network infrastructure to provide encrypted security to data locally stored within the device. Only Security Operators (SO's) that are authenticated in a pre-boot environment can access the encrypted data at rest.

The access control feature contains one or more SO's who are assigned as an authenticated system user from within the management console of ePO's command center. The access control feature contains information about the Customer's SO only for the purpose of authentication within the pre-boot phase. Trellix Drive Encryption captures data to perform authentication and security features and to enforce Customer security policies.

- **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 ePO On - Prem server/database present within the Customer's network infrastructure.

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

Table 1. Personal Data Processed by Trellix Drive Encryption

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● User Question & Answer ● User Name ● User Display Name ● User Distinguished Name ● User Account Control ● User SAM Account Name ● User Domain Name	Required to enable product functionality (access control, recovery). Required for product diagnostics.

	● User Certificate(s) ● User ID ● User Group(s) / OU(s) ● Group ID ● Group Name	
Generated Data	Incidents / Events / Logs: ● Trellix Agent GUID ● System Model ● System Manufacturer ● User Name ● User Object ID ● Policy ID	Required for product diagnostics and auditing.
Collected Data	Configuration information: ● User AD credentials ● User Question & Answer ● User Name ● User Display Name ● User Distinguished Name ● User Account Control ● User SAM Account Name ● User Domain Name ● User Certificate(s) ● User ID ● User Group(s) / OU(s) ● Group ID ● Group Name	Required to enable product functionality (access control, recovery, password synchronization, Single Sign-On).

***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 ePO - On-Prem managed deployments, the data center is located within the Customer's network infrastructure.

Subprocessors

Trellix partners with service providers that act as subprocessors for the Drive Encryption 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 Categories	Service Type	Location of Data Center
Not Applicable	Not Applicable	Not Applicable	Not Applicable

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 Drive Encryption to carry out the service, who can access that data, and why.

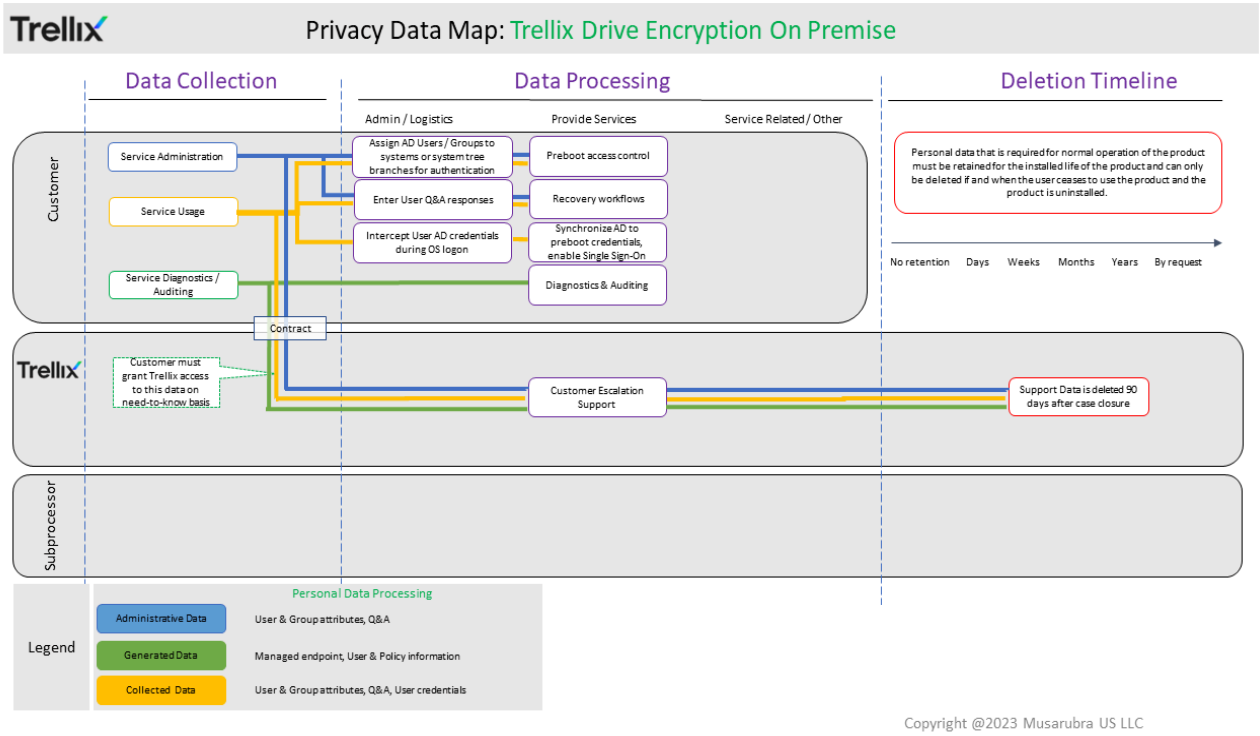
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Required for product functionality. Access limited to Customer administrators in accordance with Customer policies and controls.

	Trellix	No default access. Debugging of the Customer data in the event of an escalation.
Generated Data	Customer	Required for product diagnostics and auditing. Access limited to Customer administrators in accordance with Customer policies and controls.
	Trellix	No default access. Debugging of the Customer data in the event of an escalation.
Collected Data	Customer	Required for product functionality. Access limited to Customer administrators in accordance with Customer policies and controls.
	Trellix	No default access. Debugging of the Customer data in the event of an escalation.

Trellix Drive Encryption 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, 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 Drive Encryption 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 can forward the personal data processed by Drive Encryption 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., 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 Drive Encryption, 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 5a. Data Retention

Personal Data Category	Retention Period	Reason for Retention
Administrative Data	Not Applicable	Not Applicable
Generated Data	Not Applicable	Not Applicable
Collected Data	Not Applicable	Not Applicable

Personal data that is required for normal operation of the product must be retained for the installed life of the product and can only be deleted if and when the user ceases to use the product and the product is uninstalled.

Data written to log files on the endpoint are overwritten based on a policy whereby log files are recycled once they reach a predetermined size. The time for which the data might persist is therefore not predictable. However, the administrator can remove the logs at any time, although in such a case the product will recreate the log files and continue to write data thereafter.

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
Generated Data	See Table 1	Encrypted in transit
Collected Data	See Table 1	Encrypted in transit

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 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.

The information provided with 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.