Trellix Privacy Data Sheet We bring security to life.

Trellix File & Removable Media Protection On-Premises (FRP - On-Prem) with Optional Mobile Device Application

The purpose of this Privacy Data Sheet is to provide Customers of Trellix File & Removable Media Protection On-Premises (FRP - 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 FRP - On Prem 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 FRP - On-Prem subscription.

Trellix will process personal data from FRP - 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 FRP - On-Prem to provide its functionality.

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

Product Overview

Trellix FRP On-Prem delivers policy-enforced, automatic, and transparent encryption of files and folders stored or shared on PCs, file servers, cloud storage services, emails, and removable media such as USB drives, CD/DVDs, and ISO files. FRP - On-Prem also provides support for Removable Media initialization for Mac client systems.

FRP - On-Prem ensures that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved. You can create and enforce central policies based on users and user groups for specific files and folders, without user interaction.

[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."

FRP - On-Prem allows you to:

- Encrypt or block writes to removable media at VDI workstations;
- Access encrypted data anywhere, without any additional software installation or local administrative rights on the device host;
- Keeps files and folders secure wherever they are saved, including local hard disks, file servers, removable media, and cloud storage such as Box, Dropbox, Google Drive, and Microsoft OneDrive.

FRP - On-Prem consists of the following features:

- **Centralized management** — Provides support for deploying and managing FRP - On-Prem using Trellix ePO software;
- **User Personal Key** — A unique encryption key is created for each user;
- **Delegated administration through Role Based Key Management** — Enables the logical separation of management between multiple administrators. This capability is critical for separation across business functions and subsidiaries;
- **Key management and policy assignment auditing** — Key management and policy assignment actions performed by Trellix ePO administrators are recorded in the Audit Log. This feature is critical to ensure compliance and prevent abuse by privileged administrators;
- **Protection of data on removable media** — Enables encryption of removable media and access to encrypted content, even on systems where FRP - On-Prem is not installed;
- **Network encryption** — Enables secure sharing and collaboration on network shares.
- **User-initiated encryption of files and email attachments** — Allows users to create and attach password encrypted executable files that can be decrypted on systems where FRP - On-Prem is not installed;
- **USB removable media and CD/DVD/ISO event auditing and reporting** — Captures all user actions related to USB removable media and CD/DVD/ISO events. The auditing capability provides an effective feedback loop for administrators making policy decisions;
- **Integration with the Trellix tray icon** — Consolidates the tray icons into one common Trellix icon.
- **Use of Trellix Common Cryptographic Module (MCCM)** — FRP - On-Prem uses the MCCM user and kernel FIPS 140-2 cryptographic modules. You can install FRP - On-Prem in FIPS mode.

Trellix File & Removable Media Protection includes optional mobile device application:

➢ **Trellix Endpoint Assistant (Trellix EA)** is an application for mobile devices that allows users to securely access FRP encrypted files on their mobile devices.

Trellix File and Removable Media Protection can be implemented as a managed deployment:

✔ **Trellix File and Removable Media 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 systems within their organization.

Please see File & Removable Media Protection for additional information related to the Trellix File and Removable Media Protection solution.

Please also see Trellix ePolicy Orchestrator On Premise (ePO - On-Prem) Privacy Data Sheets for additional information.

Personal Data Processing

FRP - On-Prem is managed by the Trellix ePO - On-Prem platform which enables centralized policy management and enforcement for Customers' endpoints and enterprise security products. FRP - On-Prem ensures that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved. You can create and enforce central policies based on users and user groups for specific files and folders, without user interaction.

- **Trellix ePolicy Orchestrator On Premises (ePO On - Prem) deployment:** FRP captured information is sent automatically via Trellix Agent by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - Prem) server/database present within the Customer's network infrastructure.

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

Table 1. Personal Data Processed by File & Removable Media Protection On-Premises

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● Username (ePO Administrator) ● User ID ● User SID ● User DN ● Ldap DN ● Logged on domain\user ● AD password ● Preboot password ● Email Address ● AD user name ● AD user display name ● AD email address ● AD directory ID ● Initialisation password ● Recovery password ● Computer Name ● Computer ID ● Mobile Device Model	Required for product functionality, reporting, troubleshooting and diagnostics.

	• IP Address of Mobile Device • MEA Filename • FRP Encryption Key Name	
Generated Data	Events: • Removable Media ○ Recovery Key ○ Device ID ○ User ID • Key Authentication ○ Key ID ○ User ID Logs: • Audit Logs • Diagnostic Logs	Required for product functionality, diagnostics, auditing & reporting.
Collected Data	Configuration information: • GroupId • Group Name • Policy Name • Policy ID • Key ID	Required for product functionality, diagnostics, auditing & reporting.

*****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

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. 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.

For Trellix managed FRP - On-Prem deployment, all data is stored within the Customer's network infrastructure.

Table 2. Data Center Locations

Data Center Provider	Data Center Location
Not Applicable	**Not Applicable**

Subprocessors

Trellix partners with service providers that act as subprocessors for the FRP - On-Prem 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	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 on role and job function. 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 is required.

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

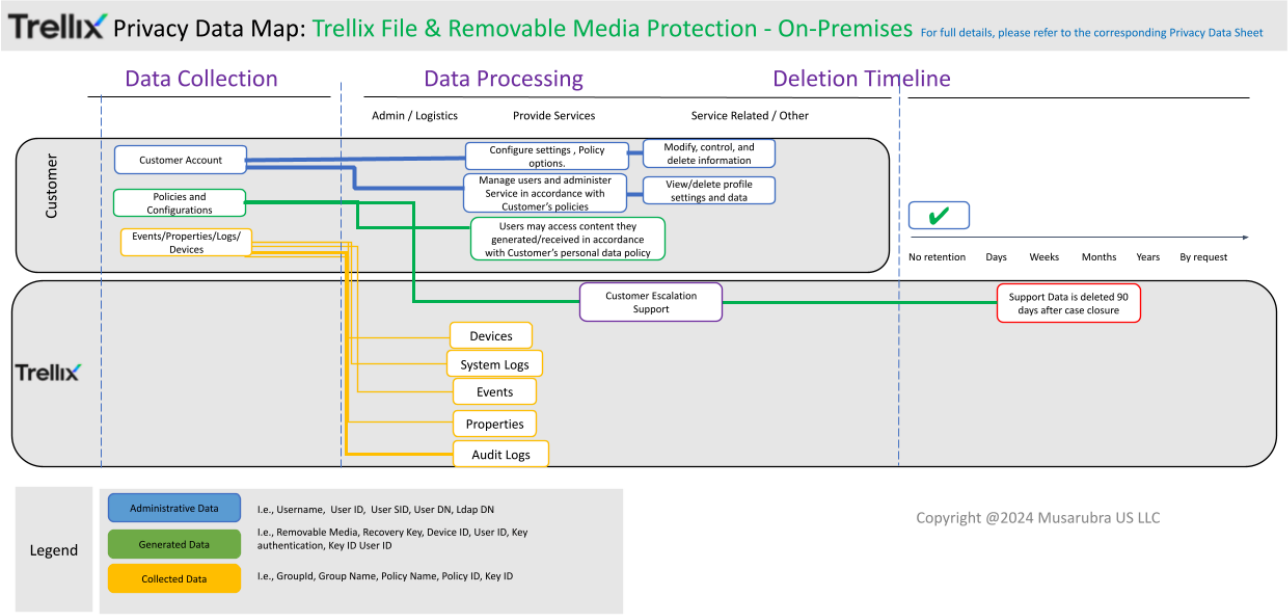
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative	Customer	Required for product functionality (policy management, enforcement & Key management). Access

		limited to Customer administrators in accordance with Customer policies and controls.
	Trellix	Debugging of customer/operational data in the event of an escalation.
Generated	Customer	Required for product functionality (user, device & key management), recovery, reporting & auditing capabilities.
	Trellix	Debugging of Customer/operational data in the event of an escalation.
Collected	Customer	Required for product functionality, reporting & auditing capabilities.
	Trellix	Debugging of customer/operational data in the event of an escalation.

Trellix File and Removable Media Protection - On-Prem 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 FRP - On-Prem 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 FRP - 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., 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 FRP - On-Prem, 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	Not Applicable.	Not Applicable.
Generated Data	Data submitted to Trellix for the purpose of troubleshooting during a support case is retained for 90 days.	To analyze a support case.
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 operates 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 Privacy 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.