

---

### Trellix Email Security - Cloud

The purpose of this Privacy Data Sheet is to provide Customers of Trellix Email Security - Cloud with details on how Trellix captures, processes, and stores<sup>1</sup> telemetry information, including personal data (or personally identifiable information), to help them understand and assess the impact of the telemetry capabilities and the overall privacy posture.

Trellix Email Security – Cloud offers industry-leading detection to identify, isolate, and immediately stop ransomware, business email compromise, spear phishing, impersonation, and attachment-based attacks before they enter the Customer’s environment. Trellix Email Security – Cloud also scans outgoing email traffic for advanced threats, spam, and viruses, and is provided to companies or persons who obtain a Trellix Email Security – Cloud subscription.

Trellix will process personal data from Email Security – Cloud 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 Email Security - Cloud to provide its functionality.

This Privacy Data Sheet is a supplement to the [Trellix Website Privacy Notice](#).

### Product Overview

Trellix Email Security - Cloud is a solution which helps organizations minimize the risk of breaches by blocking inbound and outbound malware, phishing URLs, impersonation techniques, and spam attempts. Trellix Email Security - Cloud provides an integrated, extensible security platform where Security Operations (SecOps) teams can search through threat data via the Email Security - Cloud console by way of the Email Trace functionality made available by the service. This occurs within the Customer’s email systems, allowing visibility into an organization’s email activity and threat position.

---

<sup>1</sup> 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 Email Security - Cloud detects and prioritizes high-impact email-based threats including ransomware, business email compromise, credential and spear phishing, impersonation, and URL and file-based attacks. The service leverages AI-driven security analytics, customized real-time detections, and curated contextual intelligence to eliminate known and unknown threats.

Trellix Email Security - Cloud utilizes proprietary machine learning techniques to automate URL-based threat detection, identify phishing, and filter spam. Further, it automatically flags malicious emails, helping to ensure that email administrators are promptly notified when a suspicious email enters the email stream. For more information on how Trellix implements AI or ML within our products, please see our [Artificial Intelligence and Machine Learning Data Sheet](#).

Trellix Email Security - Cloud provides Customers with effective cloud-based email threat prevention and response to rapidly stop cyberattacks and keep organizations safe. Chief Information Security Officers (CISOs) and SecOps teams rely on Trellix Email Security - Cloud for insightful visibility, improved detection effectiveness, immediate automated responses, and to mitigate attacks.

Trellix's cloud-driven detection engine, machine learning, AI, and correlation engines combine with event data from other Trellix solutions to detect, capture, and learn about the latest intelligence on cyber threats; discover malware-based threats by exposing hidden patterns and anomalies in data; index, archive, search and analyze possible malware in alerts and event data from all email sources across the Customer's organization; and integrate and improve any security operations whether located on premise, in the cloud, or in a hybrid environment.

Customers are provided with the option to easily integrate Trellix Email Security - Cloud with their email infrastructure using synchronous inline integration as well as asynchronous API integration.

Please also see [Trellix Email Security - Cloud](#) for additional information related to the Trellix Email Security – Cloud solution.

## Personal Data Processing

Information captured by the Email Security - Cloud service identifies and detects known and unknown threats across the Customer's email systems. Trellix Email Security – Cloud, paired with Trellix's cloud-based advanced threat detection engine, provides a comprehensive enterprise communication and collaboration security solution, spanning email infrastructure, enterprise applications, and collaboration platforms, helping to ensure that people can work together securely across the extended enterprise.

Trellix Email Security - Cloud provides Customers with threat detection and email event tracing capabilities. Trellix Email Security - Cloud captures email attributes, indexes the attributes, then stores them within Trellix's instance in Amazon Web Services (AWS). The captured information is made accessible to SecOps teams by allowing authenticated access to the Trellix Email Security - Cloud Web Portal and Rest APIs and provides links to identified threat artifacts when associated with an alert.

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

**Table 1. Personal Data Processed by Trellix Email Security - Cloud**

| Personal Data Category*    | Types of Personal Data Processed                                                                                                                                                                                                                        | Purpose of Processing                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Administrative Data</b> | <u>General Identification Information:</u> <ul style="list-style-type: none"> <li>• User Name</li> <li>• Email Address</li> <li>• Full Name</li> <li>• Phone Number</li> <li>• Source IP Address</li> </ul>                                             | Activation of service.<br>Authentication/Authorization.                                                               |
| <b>Generated Data</b>      | <u>Incidents / Events:</u> <ul style="list-style-type: none"> <li>• Alerts</li> <li>• Quarantine Emails</li> <li>• Email Trace</li> <li>• User Audit Logs</li> </ul> <u>Evidence:</u> <ul style="list-style-type: none"> <li>• File Contents</li> </ul> | Email event tracing and alert investigation.                                                                          |
| <b>Collected Data</b>      | <u>Configuration Information:</u> <ul style="list-style-type: none"> <li>• Original Emails</li> <li>• Recipient Address</li> <li>• Sender Address</li> <li>• Source IP Address</li> </ul>                                                               | Email analysis and verdict, compliance, debugging and troubleshooting. Security Operator review of suspicious emails. |

\* 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 Email Security - Cloud processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Canada, Japan, Ireland, and the European Union. Trellix's regional clouds provide options to address Customers' data location preferences. Customers must select a region for data processing.

**Table 2a. Data Center Locations**

| Data Center Provider | Data Center Location |
|----------------------|----------------------|
| AWS                  | AWS West (Oregon)    |
| AWS                  | AWS East (Virginia)  |
| AWS                  | Canada (Central)     |
| AWS                  | Japan (Tokyo)        |
| AWS                  | Ireland              |
| AWS                  | Germany (Frankfurt)  |

## Subprocessors

Trellix partners with service providers that act as subprocessors for the Trellix Email Security - Cloud service and contracts 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          | Table 1                | Hosting      | AWS West (Oregon)                                                                                                                                |
| AWS          | Table 1                | Hosting      | AWS East (Virginia)                                                                                                                              |
| AWS          | Table 1                | Hosting      | Canada (Central)                                                                                                                                 |
| AWS          | Table 1                | Hosting      | Japan (Tokyo)                                                                                                                                    |
| AWS          | Table 1                | Hosting      | Ireland                                                                                                                                          |
| AWS          | Table 1                | Hosting      | Germany (Frankfurt)                                                                                                                              |
| Pendo.io     | Table 1                | Analytics    | Google Cloud Platform (United States: Iowa, South Carolina, Northern Virginia, Columbus, Dallas, Oregon, Los Angeles, Salt Lake City, Las Vegas) |

## 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 Trellix Email Security - Cloud to carry out the service, who can access that data, and why.

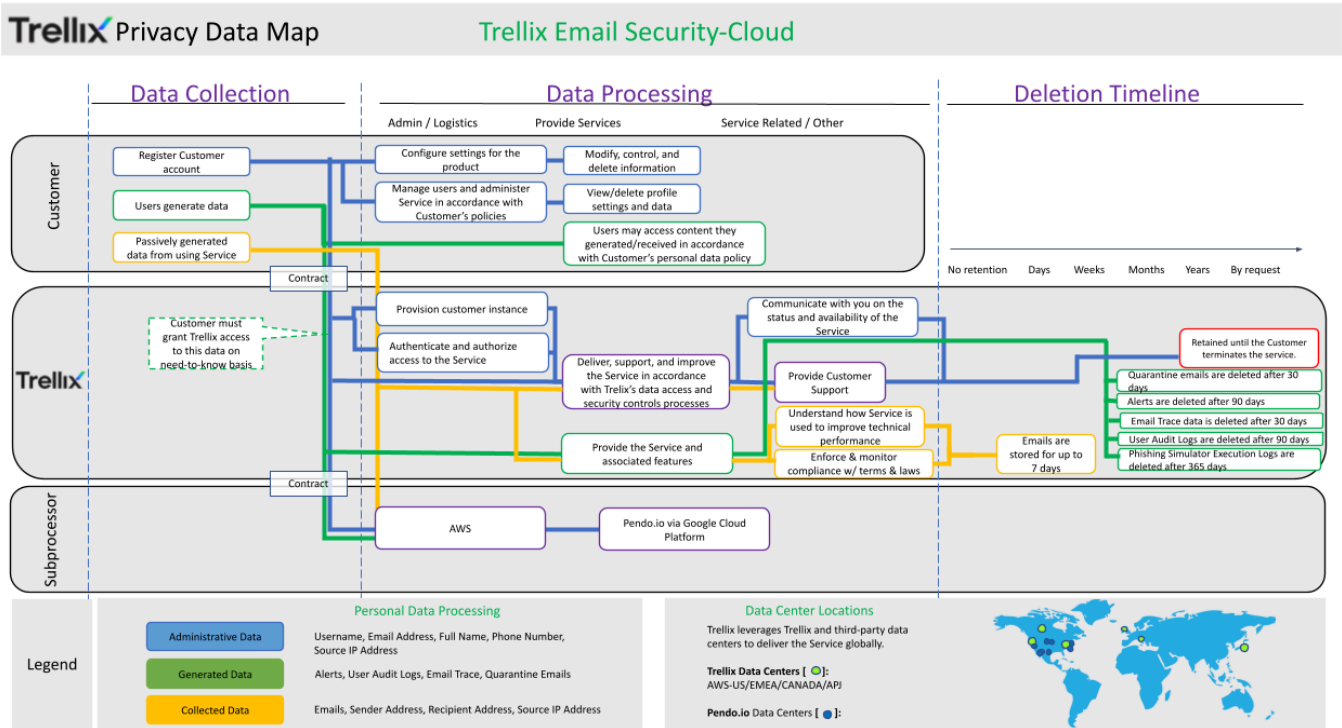
**Table 4. Access Control**

| Personal Data Category                                   | Who has access                                                                                                                                                                                                   | Purpose of the access                                                                                             |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Administrative Data (General Identification Information) | Customer:<br>Trellix Email Security – Cloud provides the capability of user access control to limit access to the data.<br>The admin tenant of the Customer can use role-based access to grant selective access. | Analysis of systems and Customer access for compliance, audit and reporting.                                      |
|                                                          | Trellix:<br>Access is available to Customer Support, Engineering and DevOps under strict guardrails.                                                                                                             | Troubleshooting of Customer environment and configuration by request from the Customer.                           |
| Generated Data (Events, Incidents and Evidence)          | Customer:<br>Trellix Email Security – Cloud provides the capability of user access control to limit access to the data.<br>The admin tenant of the Customer can use role-based access to grant selective access. | Debugging and Troubleshooting for an alert or an incident related to email security.                              |
|                                                          | Trellix:<br>Access is available to Customer Support, Engineering and DevOps under strict guardrails                                                                                                              | Debugging and Troubleshooting for an alert or an incident after it has been escalated by the Customer to Trellix. |
| Collected Data (Configuration information)               | Customer:                                                                                                                                                                                                        | Analysis of systems and Customer access for                                                                       |

|  |                                                                                                                                                                                                                |                                                                                                   |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
|  | <p>Trellix Email Security – Cloud provides the capability of user access control to limit access to the data.</p> <p>The admin tenant of the Customer can use role-based access to grant selective access.</p> | <p>compliance, audit and reporting.</p>                                                           |
|  | <p>Trellix:</p> <p>Access is available to Customer Support, Engineering and DevOps under strict guardrails.</p>                                                                                                | <p>Troubleshooting of Customer environment and configuration under request from the Customer.</p> |

Trellix Email Security - Cloud 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 Trellix Email Security - Cloud 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 Email Security - Cloud 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 Email Security - Cloud, 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 opening a case through the [Trellix Thrive portal](#). 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 terminates the service. | To authenticate the Customer's Security Operator. |
| Generated Data (Quarantine emails) | 30 days.                                            | To investigate the source of the threat.          |
| Generated Data (Alerts)            | 90 days.                                            | To investigate the source of the threat.          |

|                                                    |           |                                                                 |
|----------------------------------------------------|-----------|-----------------------------------------------------------------|
| Generated Data (Email Trace)                       | 30 days.  | To investigate the source of the threat and debugging.          |
| Generated Data (User Audit Logs)                   | 90 days.  | To investigate the source of threat and compliance.             |
| Generated Data (Phishing Simulator Execution Logs) | 365 days. | To investigate historical simulation trends.                    |
| Collected Data (Emails)                            | 7 days.   | To remediate loss of original emails and for forensic research. |

## 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.

Email Security - Cloud uses a secure portal hosted by AWS to store product 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 <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 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

2611 Internet Blvd, Suite 200

Frisco, Texas, 75034

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, 2nd Floor, Suite 2200

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, Shibuya-ku, Tokyo 150-0043

## **About This Privacy Data Sheet**

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

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.