

Talend's Assessment under CJEU Schrems II: Compliance with EU International Data Transfer Requirements

The Court of Justice for the European Union (CJEU) decision Schrems II of July 16, 2020 (the "Schrems II Decision") invalidated the EU-US Privacy Shield Framework (Privacy Shield) but confirmed the validity of the Standard Contractual Clauses, in conjunction with an appropriate privacy assessment, as a legal mechanism to transfer personal data from the European Union (EU) to countries outside of the EU.

This document aims to answer questions we anticipate our customers may have about Talend's processing of their data as a processor, when using Talend's products and services.

Customers using Talend products and services should note that:

- Talend has provided and will continue to provide customers with overlapping protections under both the Standard Contractual Clauses (SCCs) and the Privacy Shield framework for data transfers, and will continue to abide by the E.U.-U.S. Privacy Shield principles.
- Talend Cloud services are hosted on AWS instances located in the EU, and Talend has implemented and will continue to implement adequate technical and organizational security measures that meet GDPR's standards, to protect customer data in all regions.
- Talend has designed its products and services and implemented employee training to minimize customer personal data sharing with Talend and maximize the customer's control over their own data.

How the CJEU's judgement impacts cross-border personal data transfers

The Schrems II Decision invalidated the E.U.-U.S. Privacy Shield for transfers of personal data to the US from the European Economic Area countries moving forward. In its decision, the CJEU confirmed the validity of the Standard Contractual Clauses (SCCs), which are contracts approved by the European Commission for cross-border personal data transfers.

SCCs remain a valid mechanism to protect customer personal data transferred to or accessed from non-EU countries. However, the CJEU ruling advised that SCCs must be considered on a case-by-case basis, in conjunction with an assessment as to whether national security laws conflict with the guarantees provided by the data importer under the SCCs. In such case, the data transfer may still take place if an adequate level of protection for transferring data can be achieved through implementation of supplemental measures.

All customers should be assured that Talend products and services are implemented with what we consider to be adequate measures to protect customer data when accessed from locations outside of the EU, as further explained in this document.

The CJEU did not specify what these supplemental measures might be, and we are waiting to hear from the European Data Protection Board on this point. In addition to providing continuing support for our customers who need data to flow to the US, we are also continually monitoring the European Commission's and the U.S. government's reactions to the issues raised by the Schrems II Decision.

Limited Talend access to customer data

Per Talend's privacy-by-design led approach, our products and services are designed to limit the transfer of data to Talend to what is absolutely necessary for Talend to provide services. Thus, for some products configurations and services, no personal data is transferred to Talend systems at all, as further described below.

Transfer of customer data to Talend systems depends on the product configuration selected by the customer

- **For on-premises configurations, Talend software resides on customer's infrastructure, and all customer data remains within the customer's environment and systems at all times.**

Most Talend products can be installed and hosted on the customer's premises, in which case the data is stored at all times within the customer's environment and systems, and is protected by the customer's own security controls.



- **For cloud customers with hybrid configurations or remote engine configurations, the Talend software resides on customer's infrastructure, and customer data remains within the customer's environment and systems at all times**

At the choice of the customer, some components of our products can be installed in a hybrid configuration, in which case the customer's data will reside entirely on the customer's infrastructure. The hybrid configuration for Talend Cloud is further described [here](#).

- **For cloud customers using a fully managed configuration (non-hybrid), customer data may be transferred to Talend systems depending on the Talend Cloud Services components used.** Schedule A of this document identifies the Talend Cloud Services components where customer data may be transferred to Talend Cloud. For these components, please note that:
 - o **No physical transfer of EU customer data outside of the EU:** Talend Cloud services for EU customers are hosted on Amazon Web Services' SSAE 16 certified data centers. Talend Cloud AWS's primary data center is located in Germany, while back-up is in Ireland. Thus, EU customer data is stored in the EU at all times.
 - o **Customers retain full control of the data transferred to Talend Cloud:** Customers may delete their data from Talend Cloud at any time.
 - o **Access to the Talend Cloud production environment is limited to our Site Reliability Engineering and Information Security teams, which abide by strict data access policies:** Talend secure infrastructure is a closed network protected by multi-factor authentication and is accessible only to qualified members of our Site Reliability Engineering (SRE) and Information Security teams. All members of our SRE and Information Security teams have signed non-disclosure agreements and receive regular data privacy and security training.

Regardless of product configuration, customers may voluntarily provide Talend with access to customer data in the context of troubleshooting or support cases

Talend provides support and services to its customers from various locations within and outside of Europe, including from the US. Talend has implemented training and designed its products and services to minimize personal data sharing with Talend and to maximize the customer's control over their own data.

For both on-premises and cloud services, Talend offers professional services, support and troubleshooting, in the context of which customer may provide Talend with limited access to their data. These services include implementation, testing, upgrades, data migrations, and installation of additional features, functionalities, or use cases.

For all these services, the customer retains control of the means of access by Talend employees to their data, as well as on the scope and content of any data accessed by Talend.

Access to personal data or sensitive personal data for these purposes is never required. All these services can be performed by Talend employees with anonymized data. Customers should be aware of the nature and sensitivity of their data, and provide access to Talend accordingly.

In any case, Talend's access to customer data is only temporary, and any copy of customer data that may have been transferred to Talend for the purposes described therein are deleted once the services have been performed.

Talend legal mechanisms for data transfers outside the EU

Talend relies on the SCCs as a legal mechanisms to transfer EU customer personal data outside of the EU. Talend has incorporated the SCCs in its Talend Data Processing Addendum, along with the data processing clauses required under the General Data Protection Regulation and the California Consumer Privacy Act.

SCCs executed by customers remain fully valid. Our customers can continue to rely on the SCCs included in the Talend Data Processing Addendum if and when they choose to transfer their data outside the EU.

Moreover, we intend to continue to honor our Privacy Shield responsibilities as we continue to view this as an important mechanism for protecting our customers' personal data, even though Privacy Shield is no longer recognized as a valid data transfer mechanism following the Schrems II Decision.



Security

A key component of the Schrems II Decision was that SCCs should be supported by appropriate safeguards, enforceable rights for individuals and effective remedies that are needed to protect the personal data of individuals in a way that is essentially equivalent to Europe's General Data Protection Regulation.

Talend understands the importance of keeping customer data safe, and has implemented extensive security and privacy controls to supplement the protections given by the SCCs. Talend's technical and organizational security measures applicable to Talend products and services offered on the Talend Cloud are described in Schedule B of this document. As mentioned above, most Talend products can also be installed and hosted on the customer's premises, in which case customers data is stored at all times within the customer's environment and systems, and is protected by the customer's own security controls.

Government access requests

Supplemental safeguards in addition to the SCCs are, in practice, only needed if there is actually a risk of government access to data which in turn will depend on the type of personal data transferred. Not all personal data will be of interest to governmental bodies and law enforcement agencies.

In the event Talend receives a data access request from a court of competent jurisdiction or governmental body, Talend will carefully review the request, and, to the extent permitted by law, follow the steps described below:

- immediately notify the customer of the request,
- give customers the opportunity to review the request and contest the disclosure, seek a protective order, or other measures to limit data access,
- only provide access to the limited set of data for which we have a valid government access request, and not provide a governmental body with direct and unfettered access to our customers' data, encryption keys, or the ability to break our encryption.

Contacts

If you have any questions about the contents of this document, please contact us at privacy@talend.com.



Schedule A

Components	Customer Data transferred to Talend cloud?	How long does Customer Data remain on Talend systems?
Talend Management Console	<p>No</p> <p>Talend Management Console is not designed to allow transfer of customer data to Talend Cloud. However, customers may configure log files to include Customer data. Talend recommends customers to redirect log files containing their data to their own environment (cf. this Talend Community article).</p>	<p>Customers can request Talend to delete log files at any time. In any case, customer log files are automatically deleted from Talend systems after 90 days.</p>
Talend Data Inventory	<p>Yes</p> <p>Talend Data Inventory is designed to allow users to upload and store data in Talend Cloud.</p> <p>In addition, when a user adds a dataset to Talend Data Inventory which points to a remote data source (e.g., Salesforce), Talend Data Inventory retrieves a sample of the data to be stored in Talend Cloud.</p>	<p>Customers have the ability to delete the data transferred to Talend Cloud at any time.</p>
Talend Data Preparation	<p>Yes</p> <p>Talend Data Preparation is designed to allow users to upload and store data in Talend Cloud.</p> <p>In addition, sample datasets used during preparation design are stored in Talend Cloud.</p>	<p>Customers have the ability to delete the data transferred to Talend Cloud at any time.</p>
Talend Data Stewardship	<p>Yes</p> <p>Talend Data Stewardship is designed to allow users to upload and store data in Talend Cloud.</p>	<p>Customers have the ability to delete the data transferred to Talend Cloud at any time.</p>
Talend API Designer	No	N/A
Talend API Tester	No	N/A
Talend Pipeline Designer	<p>Yes</p> <p>Talend Pipeline Designer is designed to allow users to upload and store data in Talend Cloud.</p> <p>In addition, sample datasets used during pipeline design are stored in Talend Cloud.</p>	<p>Customers have the ability to delete the data transferred to Talend Cloud at any time.</p>
Talend Cloud Data Catalog	<p>No, in default mode</p> <p>However, Customers may enable the data sampling function for a specific data asset, in which case a sample of customer data is retrieved and stored in Talend Cloud.</p>	<p>Customers have the ability to delete the data transferred to Talend Cloud at any time.</p>
Cloud Engine	<p>Yes</p> <p>Cloud Engine performs job executions on a dedicated temporary resource in Talend Cloud. Data may flow through Talend Cloud during job executions.</p>	<p>The data is permanently deleted after completion of each job execution.</p>



Schedule B

Talend Technical and Organizational Security Measures applicable to Talend Cloud Services

Talend maintains technical and organizational security programs for the security, confidentiality, and integrity of the personal data it processes on behalf of its customers, as described below. Most Talend Cloud Services may be hosted either on Amazon Web Services (AWS) or Microsoft Azure (Azure), at the choice of the customer. As further described hereafter, the applicable security controls depend on whether the customer selected AWS or Azure.

Talend's technical and organizational security measures are further described in the Talend Security Architecture Overview applicable to the specific Talend Cloud Services purchased by the customer. These documents, as updated from time to time, are accessible on Talend.com or upon request.

1. Security Practices

Talend's security organization consists of a dedicated team of security experts distributed across the company who work closely with the Talend CISO. Their mission is to protect Talend and its customers through deployment of security best practices. This team supports all aspects of Talend's business. Our CISO is responsible for Talend's overall security strategy, architecture, and program.

2. Physical Security

Talend maintains security controls to prevent unauthorized physical access to buildings and data centers and to protect its systems and software, and by extension the Talend environment, from damage, interruption, misuse, or theft. Authorizations are reviewed regularly, and access is monitored continuously.

3. Security Training

All Talend employees are trained on security best practices. Talend informs all employees about relevant security procedures applicable to their respective roles, and of possible consequences of breaching security rules and procedures.

All employees involved in the development lifecycle, from creation to deployment and operation, are guided through training, reviews, and drills. For training, reviews and drills, Talend only uses anonymous data.

4. Security Software Development

The Talend security organization is involved throughout the creation of any new product application, capability, or feature. Our security experts conduct architecture, design, and code reviews. Software composition analysis (SCA) and static security vulnerability (SAST) scans are integrated into the software development lifecycle.

Talend implements a Top 10 Open Web Application Security Project (OWASP) awareness program during application development, and schedules regular internal and external audits to assess compliance with OWASP best practices.

5. Cloud workload protection and monitoring

Talend uses a combination of security services from third-party vendors to protect Talend Cloud Services.

Our security experts use external scanning tools to ensure that systems and containers are hardened, configured, and patched according to Talend guidelines and best practices.

Our deployments leverage the built-in segmentation capabilities of AWS EC2 Security groups or Microsoft Azure Network Security groups to restrict inter-resource communication.

We use web application firewalls to inspect north/south and east/west traffic flows to our applications.



Our Security Operation Center (SOC) monitors all security relevant events captured in our SIEM.

We leverage the built-in threat detection capabilities of AWS GuardDuty and Azure Advanced Threat Protection to detect malicious activity and unauthorized behavior.

6. Authentication, authorization, and access control

Standard access

Tenant users are authenticated with their own unique credentials: username plus password.

Talend uses TLS certificates issued by the Talend Certificate Authority (CA) to secure and encrypt all communications between user systems and Talend. Talend supports HTTPS over TLS.

The authentication process follows the OpenID Connect standard and uses either the authorization code or the implicit flow. Once connected, a session is managed using cookies.

Administrative access

Talend Cloud Services administrative access requires management review and approval. Elevated privilege access requires the same level of approval by management.

Access to any management console, Talend Cloud Services, AWS, or Azure requires multifactor authentication (credentials plus secret keys).

Access to the management console is restricted to select members of the Talend Site Reliability Engineering (SRE) or Information Security teams. New account creation follows a strict approval process. Accounts are reviewed quarterly.

System access is provided via Kubernetes administration management.

Password management

Talend maintains a password management policy consistent with industry standard practices that all employees must comply with. It ensures the creation of strong passwords, the protection of those passwords, and the use of a corporate password manager.

All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the Talend IT administered secret server.

7. Key management

Talend applications and components obtain and use tenant-specific Master Keys from HashiCorp Vault to encrypt tenant-related data.

Front-end TLS endpoints are managed through Traefik (Edge Router running as a Kubernetes service) and Kubernetes Secrets. Private keys are generated by Talend and certificates are signed by Talend's approved Certificate Authority (CA), GoDaddy. The certificates are then published as part of the Certificate Transparency program and uploaded to Traefik configuration as Kubernetes secrets.

8. Vulnerability management

All applications are tested by Talend security experts (dynamic application security testing (DAST) and penetration tests) at least twice a year.

In addition, Talend leverages internal and third-party security services to perform external penetration tests.

Third-party penetration tests are scheduled twice a year and prior to any new Talend Cloud Services release and deployment. The penetration tests cover a wide range of security aspects of the application and address modern web best practices.



All detected vulnerabilities are logged by the Talend Quality Assurance team and analyzed by the Talend Information Security team, which then supports, tracks, and tests their remediation.

Talend follows the Security Content Automation Protocol (SCAP) framework. Vulnerabilities are rated according to the Common Vulnerability Scoring System (CVSS) v3.0 equation. Vulnerabilities are resolved depending on their severity rating and their potential impact on the infrastructure.

9. Backups

Talend uses AWS or Azure services for both mirroring and long-term storage. All storage processes are automated, monitored, and tested. Mirrors and snapshots are performed twice daily.

10. Disaster recovery and business continuity

Talend maintains a disaster recovery/business continuity (DR/BC) policy that is reviewed, updated, and tested annually.

Talend operates in multiple AWS and Azure regions globally. Any Talend instance in any public cloud region can fail over to another region of the same public cloud vendor.

We are in close contact with both vendors and carefully monitor their service levels to make sure that they meet our required service levels.

Our development team spans six geographical locations: one in the US, four in Europe, and one in Asia. Every development function can be fulfilled by at least two developers.

Our operations team spans five geographical locations: two in the US, three in Europe, and one in Asia. Every operations function can be fulfilled by at least two members of the team.

11. Incident Response Process

Talend maintains a record of security breaches which includes a description of the breach, the time period, the consequences of the breach, the context surrounding the report of the breach, and the mitigation measures taken as a result of the breach.

For each security breach that is a Security Incident, notification by Talend to the customers will be made without undue delay.

12. Security certifications

Talend is SOC 2 Type 2 certified. Talend technical and organizational security measures are further described in Talend's current security attestation report.

Talend uses the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program to assess our security practices and validate the security posture of our cloud offerings.

Please refer to the AWS and Azure websites for more details about their security certifications and compliance information.