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

Last updated: December 2022

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 assist our customers in complying with their compliance with the EU cross-border data transfer requirements when using Talend’s products and services.

Customers using Talend products and services should note that:

- Talend currently provides customers with overlapping protections under both the Standard Contractual Clauses (SCCs) and the Privacy Shield framework for data transfers.
- Talend Cloud services are hosted on AWS instances located in the EU, and Talend has implemented adequate technical and organizational security measures that meet GDPR’s standards, to protect customer data.
- Talend takes steps 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).

SCCs remain a valid mechanism to protect the transfer of or access to customer data to 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 as long as there is an adequate level of protection for transferring the data achieved through implementation of supplemental measures.

Talend products and services are implemented with measures to protect customer data when accessed from locations outside of the EU, as further explained in this document.

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 necessary. Thus, for some products configurations and services, no personal data is transferred to Talend systems at all.

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 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:
  
  - 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 remains in the EU at all times.
  
  - Customers retain full control of the data transferred to Talend Cloud: Customers may delete their data from Talend Cloud at any time.
  
  - 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 data privacy and security trainings.

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 not generally 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 currently uses the SCCs as legal mechanisms to transfer EU customer data outside of the EU, and retains its Privacy Shield registration even though Privacy Shield is no longer recognized as a valid data transfer mechanism following the Schrems II decision. 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 other relevant data protection laws.

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.
Assessment of the United States (US) laws and regulations

The US has implemented law enforcement and state security-related legislation and executive powers that enable law enforcement and state security agencies to obtain access to personal data processed by a US-based cloud computing provider in a way that is contrary to its customers’ processing instructions. These powers include s.702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333), as further described below.

Pursuant to s. 702 FISA, the United States government (USG) can compel electronic communications service providers to disclose information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering is jointly authorised by the US Attorney General and the Director of National Intelligence, and must be approved by the Foreign Intelligence Surveillance Court in Washington, DC. Once approved, USG sends relevant providers certain “selectors” (such as telephone numbers or email addresses) associated with specific “targets” (such as a non-US person or legal entity). In-scope providers must comply with these directives in secret and are not allowed to notify their users.

Pursuant to Executive Order 12333, USG authorises intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies collect foreign “signals intelligence” information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater cables carrying Internet data in transit to the United States. EO12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

To date, however, Talend has never received an order to disclose data to US government agencies. Talend has implemented the government data access policy described below that would govern Talend’s response to any such order.

Assessment of India laws and regulations

The Telegraph Act (1885) allows the Indian government to intercept and disclose information in response to any public emergency or in the interest of public safety. The Information Technology Act (2000) allows the Indian government to access any information received or stored through any computer resource if the activity is “necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence.”

However, the India Supreme Court recognizes the right to privacy as a fundamental right under the Indian Constitution. This limits the scope of the two Indian surveillance laws referred to above. In Indian government access request must be approved by a competent authority, and the approval is subject to mandatory periodic reviews.

Talend has never been subject to an Indian government request for access to customer personal data. The lack of government access requests, in combination with the practices of the Indian authorities, India surveillance laws and regulations that are potentially applicable to Talend’s processing of personal data are unlikely to be applied in practice to customer data processed by Talend, and Talend has no reason to believe that such laws and regulations will prevent Talend from fulfilling its obligations under the SCCs.

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.

Talend maintains a Government Data Request Policy and Transparency Report, both of which are available within the Talend Security Portal.

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:

- 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.

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.

Talend sub-processors
Talend uses Sub-processors to provide ancillary services to help support, operate, and maintain Talend products and services. Depending on the product configuration chosen by the customer, the Subprocessors below may process, store, or otherwise access limited customer data or personal data in the course of providing their ancillary services. For example, Talend Cloud Services may be hosted either on Amazon Web Services (AWS) or Microsoft Azure (Azure), at the choice of the customer. Talend has entered into a data processing addendum with all of our Sub-processors which include the Standard Contractual Clauses, per which Sub-processors have undertaken to give customers’ data the same levels of security and privacy that it would receive in the EU.

A full list of Talend Sub-processors is available within the Talend Security Portal.

Contacts
If you have any questions about the contents of this document, please contact us at privacy@talend.com.
<table>
<thead>
<tr>
<th>Components</th>
<th>Customer Data transferred to Talend cloud?</th>
<th>How long does Customer Data remain on Talend systems?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Talend Management Console</td>
<td>No</td>
<td>Customer log files are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Talend Data Inventory</td>
<td>Yes</td>
<td>Customers have the ability to delete the data transferred to Talend Cloud at any time. All Customer Data are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>Talend Data Inventory is designed to allow users to upload and store data in Talend Cloud. 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.</td>
<td></td>
</tr>
<tr>
<td>Talend Data Preparation</td>
<td>Yes</td>
<td>Customers have the ability to delete the data transferred to Talend Cloud at any time. All Customer Data are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>Talend Data Preparation is designed to allow users to upload and store data in Talend Cloud. In addition, sample datasets used during preparation design are stored in Talend Cloud.</td>
<td></td>
</tr>
<tr>
<td>Talend Data Stewardship</td>
<td>Yes</td>
<td>Customers have the ability to delete the data transferred to Talend Cloud at any time. All Customer Data are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>Talend Data Stewardship is designed to allow users to upload and store data in Talend Cloud.</td>
<td></td>
</tr>
<tr>
<td>Talend API Designer</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Talend API Tester</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Talend Pipeline Designer</td>
<td>Yes</td>
<td>Customers have the ability to delete the data transferred to Talend Cloud at any time. All Customer Data are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>Talend Pipeline Designer is designed to allow users to upload and store data in Talend Cloud. In addition, sample datasets used during pipeline design are stored in Talend Cloud.</td>
<td></td>
</tr>
<tr>
<td>Talend Cloud Data Catalog</td>
<td>No, in default mode</td>
<td>Customers have the ability to delete the data transferred to Talend Cloud at any time. All Customer Data are automatically deleted from Talend systems within 31 days after contract termination.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Cloud Engine</td>
<td>Yes</td>
<td>Unless required to be retained for longer, the data are deleted within two (2) hours after completion of each job execution. The Cloud Engine used for the job is terminated as well.</td>
</tr>
<tr>
<td></td>
<td>Cloud Engine performs job executions on a dedicated temporary resource in Talend Cloud. Data may flow through Talend Cloud during job executions.</td>
<td></td>
</tr>
<tr>
<td>Stitch</td>
<td>Yes</td>
<td>If you are a Stitch customer, please see the Overview of Data Retention found here for more detail.</td>
</tr>
</tbody>
</table>


| Talend Cloud Evaluation License | Yes, to the extent the Cloud Evaluation License involves a Component that transfers data to Talend cloud. See above components. | All Customer Data are automatically deleted from Talend systems within 120 days after expiration of the evaluation period. |
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. Talend Cloud Services may be hosted either on Amazon Web Services (AWS) or Microsoft Azure (Azure), at the choice of the customer. 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. Access to an the overview of Talend Cloud Data Fabric security can be found here.

1. Security Practices

   Talend’s security organization consists of a dedicated team of security experts distributed across the company. Their mission is to protect Talend and its customers through deployment of security best practices. This team supports all aspects of Talend’s business.

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 Awareness Trainings

   Talend conducts security training programs for all employees, including, but not limited to, legal responsibilities with regard to security and data integrity and secure coding for relevant teams.

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.

   Automated security scans and testing such as Software composition analysis (SCA), SAST and DAST 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 bi-annual external audits. Talend also runs a continuous Bug Bounty program.

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.

   Talend uses the NIST Cybersecurity Framework as part of its global security strategy.

   Our deployments leverage the built-in segmentation capabilities of AWS Security groups and Microsoft Azure Security groups to restrict interresource communication.
All code is tested in Talend’s lower environments before promotion to production (DEV, QA, Staging). Production is physically and logically separate from lower environments according to the principle of segregation of duties.

Talend Cloud Data Fabric’s perimeter security is composed of, but not limited to:

- Anti-DDoS protection - prevents distributed denial-of-service attacks
- Web Application Firewall (WAF) - validates, monitors, and filters all web application and API traffic
- Network-based intrusion detection system (IDS) and intrusion prevention system (IPS) - alerts on rogue activity and protects against threats such as zero-day attacks
- Security information and event management system (SIEM) - monitors and observes system status, performance, and detects rogue processes
- Cloud Security Posture Management (CSPM) - continuously monitors cloud infrastructure to identify misconfiguration issues and compliance risks

6. Authentication, authorization, and access control

User access

Tenant users are authenticated with their own unique credentials: username plus password by default. Talend also supports integration with external SAML-based single-sign-on and multifactor authentication (MFA) providers. In addition, source IP-based access control can be applied to restrict access to Talend Data Fabric from unauthorized locations.

Talend exposes public APIs that let developers automate workflows and let auditors populate regulatory compliance reporting. Access to these APIs is secured with access tokens either bound to an individual (Personal Access Token) or bound to a programmatic client (Service Account).

Administrative access

The Cloud environment is separated from corporate IT resources and assets; only selected members of the SRE team can access the Cloud environment. New account creation follows a strict approval process. Privileged access for the Cloud environment must be requested, is time constrained, and only performed via a bastion host. Administrators receive training on their legal responsibilities with regard to security and data integrity. Account privileges are reviewed quarterly.

Audit trails

Talend Cloud Data Fabric provides an always-on audit trail capability to help monitor user activities. The audit logs are made available via a REST API. The logging service tracks all users and their actions in the system with the timestamps and outcome of those actions.


7. Key management

Talend follows best practices on encryption and key management. As audited by third-party auditors, Talend has defined policies, procedures, and controls covering the entire encryption key lifecycle such as key provisioning, rotation, destruction, and auditing.
Customer data stored on Talend infrastructure is always encrypted in transit with TLS 1.2 and at rest with minimum AES-256. A unique data encryption key (DEK) is used to encrypt tenant-specific information.

Talend relies on third-party key management services to manage the encryption key lifecycle, including key rotation.

Talend relies on trusted certificate services such as AWS Certificate Manager or Let’s Encrypt to provision, manage, and deploy SSL/TLS certificates.

**Unique Key pairing with Talend Management Console**

During the pairing process of a Remote Engine with Talend Management Console (TMC), a unique Key-Pair (RSA/4096 bits) is generated on the engine side. The public part of the key is shared to TMC for further information exchange, where it is used to encrypt any sensitive information that is sent to the remote engine.

**Job Artifact Signature**

To ensure workload integrity, Talend Studio signs task artifacts before deployment to Talend Management Console and signature verification is performed by Remote Engines prior to task execution.

8. **Vulnerability management**

Talend partners with external vendors for Static Application Security Testing (SAST) and Software Composition Analysis (SCA). The vendors scan our software for security vulnerabilities in third party or community software, and in our own code. Scans are automated and integrated in the development process of every Talend product.

Talend partners with external vendors to conduct Dynamic Application Security Testing (DAST). Scans are automatically run weekly and monthly.

Talend partners with external vendors for penetration testing against the OWASP standard. Talend also conducts a private Bug Bounty program to extensively test the security of our applications.

Vulnerabilities are analyzed by the Talend Information Security team, which then supports their remediation or mitigation.

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.

Third-party penetration test reports are available to customers upon request subject to non-disclosure agreement.

9. **Disaster recovery and business continuity**

**Recovery Strategy**

Talend’s recovery strategy is a set of predefined actions implemented in response to a business interruption from a disaster. These can be natural (earthquake, flood, hurricane, fire, etc.) or Cloud provider region-wide outages. Talend Cloud Data Fabric Disaster Recovery strategy is using the “pilot light” type approach. For faster recovery of the Cloud network infrastructure, data backends and application infrastructure are pre-provisioned at the failover region and necessary capacity reservations are set. The pilot light site infrastructure remains mostly turned off.

**Data Backup and Replication**

All Talend Cloud data backends are backed up regularly and replicated continuously to the failover region.

**Monitoring**
Talend is monitoring all data backend backups and data replication to the failover region and follows up the backup status using an internal dashboard to ensure the RPO target is respected.

The latest uptime per region is available on https://trust.talend.com.

**Testing**

Talend performs tests of the below plans:

- **Paper Test**: involved stakeholders review and update recovery plans
- **Structured Walkthrough**: step-by-step review of disaster recovery plans and configurations
- **"War Game Day" Simulation**: scenario-based practice execution of plans
- **Automatic bi-weekly backup data restoration and integrity tests**: at the failover region.

### 10. Incident Response Process

11. Talend maintains an Incident Response Team and Incident Response plan. The Incident Response team meets regularly to update and practice Talend’s incident response procedures. **Security certifications**

Talend is SOC 2, ISO 27001:2013 and ISO 27701:2019 certified and eligible to sign HIPAA (Health Insurance Portability and Accountability Act) Business Associate Agreements (BAAs).

Talend uses the following program and vendor platform to assess the security and maturity level and transparently share the ratings.

- **Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program**
- **BitSight Security Rating**
- **SecurityScorecard**
- **CyberVadis**
- **RiskLedger**

A comprehensive list of security certifications and privacy compliance is available at https://www.talend.com/security/.