Security, Privacy and Architecture of Tableau Online

Published: May 7, 2021

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's Master Subscription Agreement.

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the services provided by Salesforce that are branded as Tableau Online and licensed under Salesforce's Master Subscription Agreement (the "Covered Services").

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via a customer-specific unique identifier and allows the use of customer and user role-based access privileges. The specific infrastructure used to host and process Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is only processed as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to the processing activities provided by them. Compliance with such obligations, as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors, are subject to regular audits. The "Infrastructure and Sub-processors" documentation linked to above describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services.

Third-Party Functionality

Unless customer customizes authentication as explained below ("User Authentication"), the Covered Services use Auth0, Inc., a third-party authentication service that stores and processes certain Registration Data (e.g., email, first name, last name, and password) used to authenticate users.

Audits and Certifications

The following security- and privacy-related audits and certifications are applicable to one or more of the Covered Services, as described below:

- **EU and UK Binding Corporate Rules (BCR) for Processors**: Customer Data submitted to the Covered Services is within the scope of the Salesforce EU and UK BCR for Processors. The most current versions of the Salesforce EU and UK BCR for Processors are available on Salesforce's website, currently located at https://www.salesforce.com/company/privacy/.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Covered Services is within the scope of a Tableau's annual certification to the EU-U.S. Privacy Shield

Framework and Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce. The current certification is available at https://www.privacyshield.gov/list by searching under "Tableau."

- **System and Organization Controls (SOC) report**: Salesforce's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of System and Organization Controls (SOC) 2 type 2 and SOC 3 reports. Salesforce's most recent SOC 2 and SOC 3 reports for the Covered Services are available at https://compliance.salesforce.com.
- **APEC Privacy Recognition for Processors (PRP):** Customer Data submitted to the Covered Services is within the scope of Salesforce's PRP certification under the APEC Privacy Framework. The current certification is published in the PRP Compliance Directory at http://cbprs.org/compliance-directory/prp/.

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which may include infrastructure vulnerability, production environment and/or application security assessments.

As further described in the "Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by a third party, Amazon Web Services, Inc. ("AWS"), to host and process Customer Data submitted to the Covered Services. Information about security- and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and System and Organization Controls (SOC) reports, is available from the AWS Security website and the AWS Compliance website.

Security Controls

The Covered Services include a variety of configurable security controls. These controls may include:

- Unique user identifiers (user IDs);
- Password complexity and length requirements and controls;
- Controls to throttle access after a number of consecutive failed login attempts;
- Support for Two-Factor Authentication via a customer-provided, third-party-identity provider
- Required use of TLS certificates to secure site URL access;
- Controls to terminate a user session after a period of inactivity; and
- Configurable access controls, including to enable or disable accounts.

Security Policies and Procedures

The Covered Services maintain security policies and procedures, which may include the following administrative and technical safeguards:

- User passwords are stored using a salted hash format in the event customer chooses to use Salesforce for authentication to the Covered Services;
- Passwords are not transmitted to or from the Covered Services unencrypted
- Passwords are not logged;
- No temporary password is set when a site is created;
- OAuth tokens are encrypted and not transmitted unencrypted;
- Client-server communication logs are maintained temporarily to facilitate debugging and system monitoring.

Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Intrusion Detection
Salesforce, or an authorized third party, monitors for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs
All Salesforce systems used in the provision of the Covered Services log information to their respective system log facilities or a centralized logging service (for network systems) to enable security reviews and analysis.

Incident Management
Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.

User Authentication
Access to the Covered Services requires a valid authentication credential (e.g., valid email address and password combination or an API key/secret). Customers can choose to authenticate via a Non-SFDC Application third-party SSO and/or authentication provider (see here). Any transmission of authentication credentials to or from the Covered Services is encrypted while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security
Production data centers used to provide the Covered Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Reliability and Backup
All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. Customer Data submitted to the Covered Services is stored on a primary database server and file servers that are clustered with a backup database server and file server for higher availability. All Customer Data submitted to the Covered Services is backed up regularly.

Disaster Recovery
AWS data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. Salesforce has disaster recovery procedures in place which provide for backup of critical data and services. A system of recovery processes exists to bring business-critical systems for Covered Services back online if needed.

Viruses
The Covered Services do not scan for viruses that could be included in attachments or other data uploaded into the services by customers.

Data Encryption
The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including TLS 1.2 or newer.

Return of Customer Data
During the subscription period, customers may export a copy of any Customer Data through the Covered Services at any time. Customers are given a 14-day grace period following the expiration of their subscription period, during which they can continue to access the Covered Services and export their data. At the end of the 14-day grace period, Customer access to the Covered Services is suspended. During the 76-day period immediately following the grace period, a Customer may request export of Customer Data by contacting customer support.

Deletion of Customer Data
After termination of the Covered Services and expiration of the 90-day period described above, Customer Data submitted to the Covered Services will be deleted within 60 days. This process is subject to applicable legal requirements.

Sensitive Data
Important: The following types of sensitive personal data may not be submitted or copied to the Covered Services: payment card data; government-issued identification numbers; and financial information (such as credit or debit card numbers, bank account numbers and any related security codes or passwords).

For clarity, the foregoing restrictions do not apply to financial information provided to Salesforce for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by the website privacy statement for the applicable Covered Service.

In addition, the following types of sensitive personal data may not be submitted or copied to the Covered Services: personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, except in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission contractually. If Customer does submit personal health information or other sensitive or regulated data to the Covered Services, then Customer is responsible for ensuring that its use of such Covered Services to process that information complies with all applicable laws and regulations.

Registration Data
To access or use the Covered Services, customers must provide information about Users or system administrators ("Registration Data"). Registration Data consists of username, name, email, organization, department, job role, postal code, and phone number. Salesforce processes Registration Data, or derived information thereof, and usage data as a data controller, including for communications, internal administration, to enforce terms and conditions, and to secure, support, deliver, and provide improvements to the Covered Services. Salesforce provides appropriate protections for Registration Data and usage data and treats it consistently with the Tableau Privacy Statement.

Analytics
Salesforce may track and analyze the usage of the Covered Services for the purposes of security and helping Salesforce improve both the Covered Services and the user experience in using the Covered Services, including by tracking, using, and storing usage data for such purposes. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality. For the Covered Services, usage data may include natural language and other search queries, Registration Data, or data identifying or naming a file, Viz, folder, instance, Workbook, Worksheet, field name, filter name, label, or similar data object, including labeling provided directly by the Customer.

Salesforce may share usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis, and improvements. Additionally, Salesforce may share such usage data on an aggregate basis in the normal course of operating our business, for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services
The Covered Services may interoperate or integrate with other services provided by Salesforce or third parties. Security, Privacy and Architecture documentation for services provided by Salesforce is available in the Trust and Compliance Documentation. Salesforce also provides a variety of platforms and features that allow Salesforce users to learn about Salesforce products, participate in communities, connect third-party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Salesforce may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Salesforce may communicate with customers and their users for transactional or informational purposes; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications. Salesforce may offer customers and users the ability to deactivate or opt out of receiving such messages.