

Security, Privacy and Architecture of Customer 360 Data Manager Services

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 branded as Customer 360 Data Manager (for the purposes of this document only, the "Covered Services").

This documentation does not apply to other Salesforce services that may be associated with or integrate with the Covered Services, such as B2C Commerce/Commerce Cloud, Sales Cloud, Service Cloud, Salesforce Shield, Salesforce Connect, and Tableau CRM¹. Documentation for those services is available in the [Trust and Compliance Documentation](#).

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 customer-specific "Tenant IDs" and allows the use of customer and user role-based access privileges. The specific infrastructure used to host 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 processed only 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 their processing activities. 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 describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services.

Audits and Certifications

The Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

- **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/>.

¹ Tableau CRM refers to Services formerly branded as Einstein Analytics.

- **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/>.
- **TRUSTe certification:** Salesforce's [Website Privacy Statement](#) and privacy practices related to the Covered Services are assessed by TRUSTe annually for compliance with TRUSTe's Certification and Verification Assessment Criteria. For more information on the status of Salesforce's certification/verification status, click [here](#).

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Please see additional information on such controls in the [Salesforce Security Guide](#). Information on Multi-Factor Authentication and Single Sign-On for access to the Covered Services is set forth in the applicable Notices and License Information (NLI).

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, tokenized user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, Salesforce can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the Covered Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Trail" and are available for viewing by a customer's system administrator. Customer may copy and save this data locally.
- Salesforce personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the Covered Services 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 systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order 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.

Salesforce typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Salesforce's response.

User Authentication

Access to the Covered Services requires authentication via one of the supported mechanisms as described in the [Salesforce Security Guide](#), including user ID/password, SAML based Federation, OpenID Connect, OAuth, Social Login, or Delegated Authentication as determined and controlled by the customer. Following 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 that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity, and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to localized data stores. Backups are verified for integrity and stored in the same data centers as their instance.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable.

Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data

center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore will not damage or compromise the Covered Services by virtue of containing a virus.

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 through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers across a dedicated, encrypted link utilizing AES-256 encryption.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer). Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Salesforce uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Salesforce Security, Privacy and Architecture Documentation in the event of such a change.

Day 0, subscription terminates	Day 0 - 30	Day 30 - 120	Day 121 - 211	Day 121 - 301
	Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

Sensitive Data

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

Additionally, for the Covered Services, the following types of sensitive personal data may not be submitted: 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 the Covered Services to process that information complies with all applicable laws and regulations.

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 Salesforce's [Website Privacy Statement](#).

Analytics

Salesforce may track and analyze the usage of the Covered Services for purposes of security and helping Salesforce improve both the Covered Services and the user experience in using the Covered Services. 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.

Salesforce may share anonymous usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis and improvements. Additionally, Salesforce may share such anonymous 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 contact users to provide transactional information about the Covered Services; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications. Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.