Agentforce Supply Chain Security, Privacy and Architecture

Published: January 6, 2026

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 MSA.

Services and Features 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 and features provided by Salesforce that are branded as Agentforce Supply Chain (collectively, for the purposes of this document only, 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 unique ID. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. Further, the architecture 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 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 describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services. As described in this documentation, Amazon Web Services, Inc. ("AWS") provides architecture that supports the 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.

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

- **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/.

- **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/legal/privacy/.
- **Data Privacy Framework Certifications:** Customer Data submitted to the Covered Services is within the scope of annual certifications to the EU-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, and Swiss-US Data Privacy Framework as administered by the US Department of Commerce and further described in our Notice of Certification. The current certifications are available at https://www.dataprivacyframework.gov/s/ by searching under "Salesforce."
- **ISO 42001**: Agentforce and Einstein (AI Platform) are certified under the ISO 42001 accreditation. ISO/IEC 42001 is an international standard for Artificial Intelligence Management Systems (AIMS), providing a structured framework for organizations to establish, implement, maintain, and continually improve responsible AI practices. It is designed for entities that develop or use AI-based products and services, ensuring ethical, transparent, and accountable AI operations.
- **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.

Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (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 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 Agentforce Supply Chain Notices and License Information (NLI). As further described in the "Infrastructure and Sub-processors" documentation available here, Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process Customer Data submitted to the Covered Services. Information about security provided by AWS is available from the AWS Security Website.

Security Policies and Procedures

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

- Customer passwords are stored (if stored at all) using a one-way salted hash.
- User access log entries will be maintained, containing date, time, 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 the Customer or its ISP.
- If there is suspicion of inappropriate access, Salesforce can provide customers log entry records for use in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- 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. Customers may download and store 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.

Further information about security provided by AWS is available from the AWS Security Website.

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 for security purposes, including to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

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) 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.

User Authentication

Access to 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 systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured

by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored in cloud object storage and other subservice-provided data storage solutions, which are configured to support high availability. All Customer Data submitted to the Covered Services is backed up daily.

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. 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 within a brief period of time.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other data uploaded into the Covered 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 through Transport Layer Encryption (TLS).

Return of Customer Data

During the contract term, customers may export a copy of any Customer Data made available for export through the Covered Services. Within 30 days post contract termination, customers may request return of their respective Customer Data, to the extent such Customer Data can be copied and exported from the Covered Services and the ability to export such data is generally made available to customers, by contacting their account representative. For the Covered Services, insights, reports, and scoring may be available for manual export only.

Deletion of Customer Data

After termination of all subscriptions associated with any of the Covered Services, Customer Data submitted to the Covered Services may remain in inactive status for up to 120 days. After such period, Customer data will be overwritten or deleted within 120 days. This process is subject to applicable legal requirements.

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

Sensitive Data

Important: The following types of sensitive personal data (including images, sounds or other information containing or revealing such sensitive data) may not be submitted to the Covered Services: credit and debit

card numbers (and any related security codes or passwords), financial information[1] (such as bank account numbers), government-issued identification numbers, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and information concerning sex life.

Additionally, personal health information (including images, sounds or other information containing or revealing such sensitive data) may not be submitted to the Covered Services. 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.

PGSSI-S. To the extent Customer is subject to Article L.1111-8 (or any successor thereto) of the French public health code (Code de la Santé Publique), Customer shall abide by the Global Information Security Policy for the Healthcare Sector (PGSSI-S) pursuant to Article L.1110-4-1 (or any successor thereto) of the aforementioned code.

If Customer chooses to use the Covered Services as part of a decision-making process with legal or similarly significant effects, Customer shall ensure that the final decision is made by a human being. Customer must take account of other factors beyond the Covered Services' recommendations in making the final decision.

Analytics

Salesforce may track and analyze the usage of the Covered Services for the purposes of security and of 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.

In addition, Salesforce may use Customer Data on an aggregate basis for purposes such as research, marketing, analysis, and benchmarking, and other purposes reasonably required to develop, deliver, and provide ongoing innovation to the Covered Services. No Customer Data consisting of personally identifiable information will be shared in this manner, nor any data that would identify customers, their users, their consumers, or any individual, company or organization. By using the Covered Services, customers consent to the use and disclosure of their Customer Data in anonymized and aggregated form.

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

[1] 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 Covered Services.

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. Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.