Data.com Security, Privacy and Architecture

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 Data.com ("Data.com Services") and accessed via the Salesforce services branded as Sales Cloud, Service Cloud or Force.com. This documentation does not apply to the "Data.com Connect" product or the product branded "Jigsaw for Salesforce" or "JFS," which is no longer generally available.

Applicability to Data.com Services Accessed through Salesforce Services

To the extent the Data.com Services are accessed and used through the Salesforce services branded as Sales Cloud, Service Cloud or Force.com certain Customer Data may be transferred to the Data.com infrastructure, and accordingly, is subject to this Data.com Security, Privacy and Architecture Documentation. Additional information about the specific infrastructure used to host Customer Data and Customer Data that may be transferred to the Data.com infrastructure is described in the "Infrastructure and Sub-processors" documentation available here.

To the extent that Customer Data remains in the Salesforce services branded as Sales Cloud, Service Cloud or Force.com, the Salesforce Security, Privacy and Architecture Documentation will apply to such data.

Architecture and Data Segregation

The Data.com 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 "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. 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 Data.com Services.

Audits and Certifications

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

Customer Data submitted to Data.com 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/.

Security Controls

To the extent that Customers interact with the Data.com Services via the Salesforce services branded as Sales Cloud, Service Cloud or Force.com, the Security Controls set forth in the Salesforce Security, Privacy and Architecture Documentation will apply.

Security Policies and Procedures

To the extent that Customers interact with the Data.com Services through the Salesforce services branded as Sales Cloud, Service Cloud, or Force.com, the Salesforce Security, Privacy and Architecture Documentation will apply.

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the Data.com Services for unauthorized intrusions using network-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 to prevent fraudulent authentications, and to ensure that the Data.com Services function properly.

Security Logs

All systems used in the provision of the Data.com 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). System and application logs will be kept for a minimum period of sixty (60) days.

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 Data.com Services directly or via a Data.com API, requires a valid user ID and password combination, or an OAuth token, both of which are encrypted via TLS 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. For the Data.com Services accessed via the Salesforce services branded as Sales Cloud, Service Cloud or Force.com, or through Data.com API’s used in connection with such services, user authentication is made through such services and no additional user authentication is required for utilization of the Data.com Services.

Physical Security

Production data centers used to provide the Data.com Services have an access control system. 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, including biometrics, 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 Data.com Services is stored on a primary database server that is clustered with a backup database server for higher availability and is stored on carrier-class disk storage using redundant disks and multiple data paths. All Customer Data submitted to the Data.com Services, up to the last committed transaction, is automatically replicated on a near real-time basis at the database layer and is backed up on a regular basis. Customer Data stored on the infrastructure for the Salesforce services branded as Sales Cloud, Service Cloud or Force.com will be backed-up in accordance with the Salesforce Security, Privacy and Architecture Documentation.

Disaster Recovery

The Data.com Services' production systems are protected by a multi-tiered disaster recovery plan which provides for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database, security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after a service disruption.

Viruses

The Data.com Services do not scan for viruses that could be included in attachments or other data uploaded into the Data.com Services by customers. Uploaded attachments are not executed in the Data.com Services and therefore will not damage or compromise the online Data.com Services by virtue of containing a virus.

Data Encryption

The Data.com Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Data.com Services including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum.

Modification of Customer Data

Customer Data may be modified by Salesforce if a customer elects to use the Data.com Services to update data fields included in the Customer Data. These modifications will correspond to the data fields provided by the Data.com Services described in the Data.com Notice and License Information.

Return of Customer Data

Customer Data submitted to the Salesforce services branded as Sales Cloud, Service Cloud or Force.com shall be returned to Customer upon request in accordance with the Salesforce Security, Privacy and Architecture Documentation.

Deletion of Customer Data

Customer Data submitted to Data.com Services and Customer Data stored on the infrastructure for the Salesforce services branded as Sales Cloud, Service Cloud or Force.com will be deleted in accordance with the Salesforce Security, Privacy and Architecture Documentation.

Sensitive Data

Important: The following types of sensitive personal data may not be submitted to the Data.com Services: government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); information related to an individual's physical or mental health; information related to the provision or payment of health care; contact information for individuals located in the European Union.

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 applicable website privacy statement.

Analytics

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