Security, Privacy and Architecture of LiveMessage, myTrailhead, Salesforce Anywhere (including Quip), Salesforce.org Philanthropy Cloud, and Salesforce.org Elevate

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 LiveMessage (formerly branded as HeyWire), myTrailhead, Salesforce Anywhere (including Quip), Salesforce.org Philanthropy Cloud, and Salesforce.org Elevate (collectively, for the purposes of this document only, the "Covered Services"). MyTrailhead, Salesforce.org Philanthropy Cloud, and Salesforce.org Elevate run on the infrastructure described by this documentation and the Heroku platform, as described in the Heroku Services Trust and Compliance Documentation. Additionally, Salesforce.org Philanthropy Cloud runs in part on the Salesforce Services platform, and if a Customer chooses to connect Salesforce.org Elevate to its CRM, Salesforce.org Elevate also runs in part on the Salesforce Services platform, which are subject to the Salesforce Services Trust and Compliance Documentation.

Salesforce Anywhere (including Quip) Accessed Through Other Services

If Customer accesses the Salesforce Anywhere (including Quip) Services through another Salesforce Service, the Salesforce Anywhere (including Quip) Services runs across two different infrastructures, as described in this Documentation and the Salesforce Services Documentation. Currently, Salesforce Anywhere (including Quip) can be accessed from Salesforce Services and as such runs across the infrastructure as described in this Documentation and as described in in the Salesforce Services Documentation. This Documentation describes the back-end infrastructure used by a Salesforce Service to store and process Customer Data for Salesforce Anywhere (including Quip). The Salesforce Service, including the data stored on the Salesforce Service, the functionality and integration presented back to the Salesforce Service, and User's login to the Underlying Service, remains subject to the Salesforce Services 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 a customer-specific unique identifier 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 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

A portion of customer support for the Covered Services may be provided using a third-party technology provider, which may contemplate data, including screenshots of customers' instances of such services or attachments submitted by a customer for support, being stored with the third party.

When customers use LiveMessage to transmit or receive mobile messages, such as SMS messages, the content of those messages and related information about those messages are received by (a) aggregators – entities that act as intermediaries in transmitting mobile messages or provisioning mobile numbers, and (b) carriers – entities that provide wireless messaging services to subscribers via wireless or wireline telecommunication networks. Such aggregators and carriers access, store, and transmit message content and related information to provide these functions. For over-the-top messaging services, such as Facebook Messenger, the content of messages sent or received via such service and related information about such messages are received by entities that enable such over-the-top messaging services.

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, with the exception of Salesforce.org Philanthropy Cloud, 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**[1]: Customer Data submitted to the Covered Services is within the scope of a Salesforce'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 "Salesforce."
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the Covered Services, with the exception of Salesforce.org Philanthropy Cloud, 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

[1] Services that are made generally available after July 16, 2020 will no longer be added to Salesforce's Privacy Shield Certification, including Salesforce.org Philanthropy Cloud and Elevate.

Verification Assessment Criteria. For more information on the status of Salesforce's certification/verification status, click here.

- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for Quip (except for Quip instances running on Salesforce Anywhere Virtual Private Cloud) in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party.
- **System and Organization Controls (SOC) report**: Salesforce's information security control environment applicable to Quip (except for Quip instances running on Salesforce Anywhere Virtual Private Cloud) undergoes an independent evaluation in the form of a System and Organization Control (SOC) 2 report. Salesforce's most recent SOC 2 report for Quip is available upon request from your organization's Salesforce account executive.
- **Payment Card Industry (PCI)**: For the Salesforce.org Elevate Payment Services systems, Salesforce has obtained an Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry (PCI) Data Security Standard (DSS). A copy of Salesforce's AoC is available upon request from your organization's Salesforce account executive.

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 revoke access or enable notification after a number of consecutive failed login attempts;
- Multi-Factor Authentication and Single Sign-On for access to the Covered Services as set forth in the applicable Notices and License Information (NLI);
- Utilize 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 a customer chooses to utilize Salesforce for authentication to such services;
- Passwords are not transmitted unencrypted;
- Passwords are not logged;
- No defined passwords are set;

- OAuth tokens are encrypted and not transmitted unencrypted;
- Access logs will be stored in a secured centralized host to prevent tampering;
- 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 independent third party, monitors 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 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

Except for end users accessing the Giving Pages feature of Salesforce.org Elevate, access to the Covered Services requires a valid authentication credential (e.g., valid user ID and password combination or an API key/secret), whether directly, through an API, or via a SSO authentication provider response. For certain services, customers can authenticate via a Non-SFDC Application third-party SSO and/or authentication provider. Any transmission of authentication credentials to or from the Covered Services is encrypted while in transmission. Following a successful authentication, a random session ID or authorization token 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.

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 that is clustered with a backup database server for higher availability. All Customer Data submitted to the Covered Services is backed up regularly.

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 if needed.

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. Virus scanning is available for customers of Salesforce Anywhere Shield.

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 later, TLS certificates with 1024-bit or 2048-bit or larger RSA keys, and AES-256 encryption.

Return of Customer Data

During the contract term, customers may export a copy of any Customer Data that is made available for export through the Covered Services. Except for Salesforce.org Philanthropy Cloud, Salesforce.org Elevate and Salesforce Anywhere Starter, within 30 days after termination of a Covered Service, customers may request return of their Customer Data submitted to such Covered Service by contacting customer support for the respective service or contacting Salesforce here, to the extent such data or analysis can be copied and exported from the Covered Services and the ability to export such data is made generally available to customers. For Salesforce.org Philanthropy Cloud, Salesforce.org Elevate and Salesforce Anywhere Starter, customers may request return of their Customer Data within 30 days after termination by logging a case here, subject to the same restrictions above.

Deletion of Customer Data

After termination of the Salesforce Anywhere (including Quip) services, Customer Data submitted to such service is retained on inactive status for 120 days, after which it is securely overwritten or deleted from production and backups within 30 days. For all other Covered Services, after termination of such service, please contact customer support or contact us here to request deletion of Customer Data submitted to the applicable service.

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 Security, Privacy and Architecture Documentation in the event of such a change.

Sensitive Data

Important: For the Covered Services, the following types of sensitive personal data may not be submitted or copied to the Covered Services: government-issued identification numbers; and financial information (such as credit or debit card numbers, bank account numbers and any related security codes or passwords). Notwithstanding the foregoing, payment card data and bank account information may be submitted to Salesforce.org Elevate where Salesforce has permitted the submission contractually. End users may submit payment card data to Salesforce.org Philanthropy Cloud, but that data is processed

through a third party as described in the Salesforce.org Philanthropy Cloud and Elevate Notices and License Information Documentation here.

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 the website privacy statement for the applicable Covered Service.

Geographic Limitation

Important: At this time, Salesforce.org Philanthropy Cloud is only available in the U.S. and Canada. Salesforce.org Philanthropy Cloud is not appropriate for use with personal data subject to the European Union General Data Protection Regulation (GDPR) or similar laws, including those of the European Economic Area, Switzerland, and the United Kingdom.

Therefore, Customers may not use Salesforce.org Philanthropy Cloud, or store or otherwise process Customer Data in Salesforce.org Philanthropy Cloud, in any way that brings such storage or processing under the jurisdiction of E.U. Law and the application of the GDPR, pursuant to Articles 2 and 3 of that law. This includes, without limitation or exclusion:

- Processing any personal data of or about residents or citizens of the European Economic Area, Switzerland, or the United Kingdom;
- Providing Salesforce.org Philanthropy Cloud access or accounts to residents or citizens of EEA countries, Switzerland, or the United Kingdom; or
- Performing any data processing involving Salesforce.org Philanthropy Cloud in the context of activities of Customer's establishment within the EEA. Switzerland, or the United Kingdom, regardless of whether the data processing itself took place within the EEA, Switzerland, or the United Kingdom.

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 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. When third-party systems connect to the Covered Services, these external systems may supply metadata to the Covered Services for the purpose of maintaining the intended functionality of the integration, for example, an external system may supply a third-party record ID, file name, folder name, or similar label intended to identify a record that is being sent to the Covered Services. Salesforce may collect and store such metadata to ensure product functionality, and to assist in debugging, support and for security purposes. Salesforce provides appropriate protections for such metadata and treats it consistently with our Privacy Statement. 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 offers customers and users the ability to deactivate or opt out of receiving such messages.