Security, Privacy and Architecture of Desk.com, Einstein Discovery Classic, LiveMessage, Quip, myTrailhead, and SalesforceIQ CRM

Published: September 6, 2019

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 Desk.com, Einstein[1] Discovery Classic (provisioned before October 16, 2018), LiveMessage (formerly branded as HeyWire), Quip, myTrailhead, and SalesforceIQ CRM (collectively, for the purposes of this document only, the "Covered Services"). MyTrailhead runs on the Heroku platform. The Einstein Analytics Plus and Einstein Prediction services are subject to the Einstein Analytics, Einstein Discovery, and "Sales Cloud Einstein, Salesforce Inbox, Einstein Engagement Scoring, Einstein Bots, and Einstein Vision and Language" documentation. The Messaging product (available only in Lightning) is subject to the Salesforce Services Trust and Compliance Documentation. Documentation for those services, including Heroku, is available in the Trust and Compliance Documentation.

For Customers who provisioned the Einstein Discovery Service before October 16, 2018, nothing has changed, and your Einstein Discovery Classic Services are subject to this documentation. For Customers who provisioned the Einstein Discovery Service on or after October 16, 2018, your use of Einstein Discovery is subject to the new "Einstein Analytics and Einstein Discovery" 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

[1] Rights of ALBERT EINSTEIN are used with permission of The Hebrew University of Jerusalem. Represented exclusively by Greenlight.

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-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Quip and Einstein Discovery 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."
- **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 Criterias. 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 SalesforceIQ CRM, Quip (except for Quip Virtual Private Cloud) and Einstein Discovery Classic 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. The scope of Salesforce's ISO 27001/27017/27018 certification applicable to SalesforceIQ CRM, Quip and Einstein Discovery Classic is available here.
- **Service Organization Control (SOC) report**: Salesforce's information security control environment applicable to Quip (except for Quip Virtual Private Cloud) undergoes an independent evaluation in the form of a Service 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.

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 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. 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;
- Two-Factor Authentication or OAuth for access to the services;
- Utilize SSL 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 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) 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 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 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

Desk.com, and LiveMessage, Quip, myTrailhead, and SalesforceIQ CRM do not scan for viruses that could be included in attachments or other data uploaded into the services by customers. Einstein Discovery utilizes software and other security measures to prevent the services from containing or transmitting viruses or other malicious code. Such measures include, but are not limited to, operating system patching, firewall or network-level detection, and security controls to prevent unauthorized installation of software.

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.x, 256-bit TLS certificates, 128 SSL certificates, 256-bit AES encryption, 1024-bit RSA public keys, or 2048-bit RSA public keys.

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; for Quip, this is applicable to enterprise customers only. Within 30 days after termination of a Covered Service, customers may request return of their Customer Data submitted to such Covered Service, or a copy of any analysis made from Customer Data through Einstein Discovery, 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 generally made available to customers.

Deletion of Customer Data

After termination of the Einstein Discovery or Quip services, Customer Data submitted to such service is retained on inactive status in back-up within the respective services for 90 days for Einstein Discovery and 120 days for Quip, after which it is securely overwritten or deleted. Salesforce may delete Customer's SalesforceIQ CRM data 30 days after contract termination. 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: 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).

Information related to an individual's physical or mental health, and information related to the provision or payment of health care, may not be submitted to the Covered Services. Notwithstanding the foregoing, such data may be submitted to Quip in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission contractually. Please contact your account manager for further information regarding submission of sensitive personal data to Quip.

Customer shall not use Einstein Discovery for the purposes of predicting an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, criminal convictions, disability, health status or medical condition.

If Customer chooses to use Einstein Discovery 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 takes account of other factors beyond Einstein Discovery's recommendations in making the final decision.

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.

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. 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. 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.