Security, Privacy and Architecture of Sales Cloud, Service Cloud, Experience Cloud (formerly Community Cloud), Chatter, Lightning Platform (including Force.com), Site.com, Database.com, Tableau CRM (including Einstein Discovery and Salesforce Data Pipelines), Einstein Relationship Insights, Messaging, Financial Services Cloud, Health Cloud, Sustainability Cloud, Consumer Goods Cloud, Manufacturing Cloud, Service Cloud Voice, Salesforce CPQ and Salesforce Billing, Customer 360 Audiences, Salesforce Maps, and Advertising Studio

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 following services (collectively, for the purposes of this document only, the "Covered Services"), as operating on Salesforce Unified Cloud (Hyperforce):

(1) Salesforce Services branded as:
- Chatter,
- Experience Cloud (formerly Community Cloud),
- Database.com,
- Lightning Platform (including Force.com, but excluding those provided for free as noted in (8) in the next section below),
- Sales Cloud,
- Service Cloud,
- Site.com, and

(2) the services branded as:
- Consumer Goods Cloud,
- Einstein Relationship Insights[1],

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

- Manufacturing Cloud,
- Messaging,
- Service Cloud Voice,
- Tableau CRM[2] , and

(3) the service branded as Customer 360 Audiences,
(4) the services branded as Advertising Studio, and
(5) the managed packages branded as:

- the Field Service managed package ("FSMP" formerly Field Services Lightening managed package), which is a feature of Service Cloud[4]. FSMP includes optional scheduling optimization functionality ("Click FS Optimizer"),
- Financial Services Cloud,
- Health Cloud,
- Salesforce CPQ and Salesforce Billing (together formerly branded as Salesforce Quote-to-Cash),
- Salesforce Maps, and
- Sustainability Cloud.

For purposes of clarification, this documentation also applies to the foregoing services and managed packages when sold as part of the packages branded as Employee Apps or App Cloud.

Services or Features Not Covered

This documentation does not apply as described below:

(1) Reliability, Backup, and Business Continuity, Return of Customer Data, and Deletion of Customer Data sections of this documentation do not apply to the temporary developer testing environments branded as “Scratch Orgs.”
(2) All data presented in Salesforce Connect is retrieved real-time through the Service from external data sources and are not copied into the Customer’s org, so for clarity, any terms relating to stored data contained in this documentation do not apply to such data.
(3) Customers may choose to use related products and features branded as Account Intelligence, Einstein Activity Capture, Einstein Article Recommendations, Einstein Bots, Einstein Case Classification, Einstein Object Detection, Einstein Opportunity Scoring, Einstein Prediction Builder, High Velocity Sales, Sales Cloud Einstein, Salesforce Inbox, and Service Cloud Einstein; these features run across two infrastructures, the infrastructure described by this Documentation, and the infrastructure described by the Einstein Platform Documentation, as further described in the Einstein Platform Documentation.
(4) Customers may choose to use related products and features branded as Salesforce Anywhere (including Quip); these features run across two infrastructures, the infrastructure described by this Documentation, and the infrastructure described by the Salesforce Anywhere (including Quip) Documentation, as further described in the Salesforce Anywhere (including Quip) Documentation.
(5) This documentation does not apply to other Salesforce services that may be associated with or integrate with the Covered Services, including, without limitation, B2C Commerce, IoT Cloud, LiveMessage, and Marketing Cloud. Among such services are the Tableau CRM Plus and Einstein Prediction Services which contain features that run on different infrastructures: the Tableau CRM Services runs on infrastructure described by the “Infrastructure and Sub-processors” documentation available here, and the Einstein Prediction Builder Service runs across infrastructure described in the “Infrastructure and Sub-processors” documentation available here and the Einstein Platform Documentation.

[2] Tableau CRM refers to Services formerly branded as Einstein Analytics. It includes the Einstein Discovery and Salesforce Data Pipelines features.

(6) To the extent a Covered Service is accessed through or interoperates with another Salesforce Service, certain Customer Data and/or Content may be transferred from such service to the Covered Services for processing, however such Customer Data remains subject to the Security, Privacy and Architecture Documentation applicable to such underlying product available here.
(7) Documentation describing the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to services running on non-Salesforce Unified Cloud (Hyperforce), is available here.
(8) Lightning Platform Developer Edition and its associated products and services that are provided for free.
(9) The Advertising Studio services are accessed through the ExactTarget services and run across two infrastructures, the infrastructure described by this documentation, and the infrastructure described by the sections of the Marketing Cloud Documentation applicable to the ExactTarget 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. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here, here. and 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 by Salesforce and/or independent third-party auditors designated by Salesforce.

The "Infrastructure and Sub-processors" documentation available here, here, and here describes the sub-processors and certain other entities material to Salesforce's provision of the Covered Services.

Third-Party Functionality

Certain features of the Covered Services use functionality provided by third parties. Customers may be able to disable such features. See product specific additional disclosures below for further information and Notice and License Information documentation available here for a list of the Non-SFDC Applications Customers may access in the Covered Services.

When customers use messaging features to transmit or receive 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 and WhatsApp, the content of messages sent or received via such service and related information about such messages is received by entities that enable such over-the-top messaging 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 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 exclusion of Einstein Relationship Intelligence, Messaging, and Service Cloud Voice–is within the scope of the Salesforce EU and UK BCR for Processors to the extent described therein. 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:** Customer Data submitted to the Covered Services–with the exclusion of Customer 360 Audiences, and Service Cloud Voice–is within the scope of Salesforce's annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. 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 Criteria. For more information on the status of Salesforce's certification/verification status, click here.
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the Covered Services – with the exclusion of Einstein Relationship Intelligence – 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/.

As further described in the "Infrastructure and Sub-processors" documentation available here, here, and here, Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") or Heroku to host or process Customer Data submitted to certain Covered Services and features. Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and SOC reports, is available from the AWS Security Web site and the AWS Compliance Web site. Information about security and privacy-related audits and certifications received by Heroku, including information on ISO 27001 certification and SOC reports, is available from Heroku's Security, Privacy and Architecture Documentation.

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). As further described in the "Infrastructure and Sub-processors" documentation available here, here, and here, Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") or Heroku to host or process Customer Data submitted to certain Covered Services and features. Information about security provided by AWS is available from the AWS Security website. Information about security provided by Heroku is available from Heroku's Security, Privacy, and Architecture Documentation.

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, 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 detect compromised browsers, 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.

Salesforce publishes system status information on the Salesforce Trust website. 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 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

Our public cloud providers are responsible for providing appropriate physical security measures. Further information about the physical security provided by AWS is available from the AWS website at: https://aws.amazon.com/compliance/data-center/controls/

Reliability, Backup, Business Continuity, and Disaster Recovery

Salesforce Unified Cloud (Hyperforce) is configured and deployed in a highly available[3] manner. The systems are designed to recover from failure in a minimally disruptive[4] manner. All Customer Data submitted to the Covered Services is written to persistent storage across multiple availability zones.

The Covered Services' Disaster Recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of multiple availability zones at the same time, and exclude development and test bed environments, such as the Sandbox service.

The Covered Services' Disaster Recovery processes are built on top of the standard deployment process; this ensures that Disaster Recovery is done using a well understood and continually validatable process. We will explicitly test a Disaster Recovery event at least one per year.

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. 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[5] products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS). The Customer Data is also encrypted at rest.

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, or if Customer has not already removed the managed package in which the Customer Data was stored). Salesforce shall provide such Customer Data via downloadable files using common or standard formats such as comma separated value (.csv) format and attachments in their native format. The foregoing return

---

[3] Highly available refers to the overall fashion in which the service and its underlying infrastructure is operated and deployed. Services are deployed across multiple availability zones within a region

[4] Minimally Disruptive means that the system is designed to continue operating during failure events in the infrastructure. The infrastructure is designed to recover from failure in an automated fashion.

[5] Leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys. Additionally, all data, including Customer Data, that is transmitted between operational boundaries is done via encrypted channels such as TLS or VPN links utilizing a minimum of AES-256 encryption.

of Customer Data for managed packages may not be available if the packages were removed prior to contract termination.

Deletion of Customer Data

After termination of all subscriptions associated with any of the Covered Services ("Subscription Termination"), 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 from production within 90 days.[6] Customer Data will be deleted from backups within 300 days of Subscription Termination. 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 Service. Salesforce will update this Security, Privacy, and Architecture Documentation in the event of such a change.

Sensitive Data

The following types of sensitive personal data may not be submitted to the Covered Services: government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers). Notwithstanding the foregoing, government-issued identification numbers and financial information may be submitted to those Covered Services that have a Payment Card Industry Attestation of Compliance (AOC) but only to the regions that have obtained the AOC, as described below in the Regional Audits and Certifications section of the Product Specific Additional Disclosures section below.

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 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.

[6] Some services do not keep separate copies of Customer Data for production and backup. In no event will such services retain any Customer Data beyond 300 days from Subscription Termination.

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.

Salesforce will not share Customer Data consisting of personally identifiable information, nor any data that will or could be used to identify customers, their users, their consumers, or any individual, company or organization. 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.

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 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 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.

Product Specific Additional Disclosures

REGIONAL AUDITS AND CERTIFICATIONS

- In addition to the privacy- and security-related audits and certifications applicable to the Covered Services as described in the "Audits and Certifications" section above, the following privacy- and security-related audits and certifications apply to (A) the following Covered Services: Sales Cloud, Service Cloud, Experience Cloud (formerly Community Cloud), Chatter, Lightning Platform (including Force.com, but excluding those provided for free as noted in (8) of the "Services or Features Not Covered" section, Site.com, Database.com, Tableau CRM, Health Cloud, Financial Services Cloud, Manufacturing Cloud, and Salesforce CPQ and Salesforce Billing (together formerly branded as Salesforce Quote-to-Cash); for (B) the following APAC regions, as described in the Infrastructure and Sub-processors Documentation: (i) Australia (Amazon Web Services, Inc.) for customers based in Australia using Salesforce Unified Cloud (Hyperforce), and (ii) India (Amazon Web Services, Inc.) for customers based in India using Salesforce Unified Cloud (Hyperforce):
    - **ASIP Santé certification:** Salesforce has obtained the French health data hosting certification (ASIP Santé certification) that enables Salesforce to host French health data. Salesforce's most recent ASIP Santé certification is available upon request from your organization's Salesforce account executive.

- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) 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 Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's Salesforce account executive.
- **NEN-7510**: NEN7510 provides specific controls supplementary to ISO27001 applicable to the Dutch healthcare sector and organizations processing Dutch healthcare data. Salesforce has engaged an independent third-party assessor to map the relevant NEN7510 controls against Salesforce's existing certifications and controls. Salesforce's most recent NEN-7510 report is available for download on Salesforce's compliance website.
- **Payment Card Industry (PCI):** 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. Customers must use either "Platform Encryption" for supported field types and file attachments or the "Classic Encryption" custom fields feature when storing personal account numbers ("PAN" or "credit card numbers") to benefit from Salesforce's PCI DSS AoC. Additionally, to benefit from Salesforce's PCI DSS AoC, customers should not implement the deterministic encryption option when using Platform Encryption. Information about "Platform Encryption" and "Classic Encryption" is available in the Salesforce Security Guide.

SALES CLOUD

- The Account Intelligence feature in Sales Cloud–Account Autofill, Account Logos, Account News, and Lightning News–works by sending standard fields from Customers' Account object to Salesforce's Einstein Platform infrastructure, currently hosted on AWS, where this data is matched to Content, such as news articles, made available through Sales Cloud. Customers can disable the Account Intelligence features.

SALESFORCE MAPS

- For Salesforce Maps, all Customer Data submitted to AWS (with the exception of data submitted through the Salesforce Maps Web Interface ("Self-Hosted Data")) is retained in AWS for 90 days, after which it is securely overwritten or deleted.

CUSTOMER 360 AUDIENCES

- In addition to the data types listed in the "Sensitive Data" section above, the following types of sensitive personal data may not be submitted to Customer 360 Audiences: racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade-union membership.
- In addition to the privacy- and security-related audits and certifications applicable to Customer 360 Audiences as described in the "Audits and Certifications" section above, the following privacy- and security-related audits and certifications apply to Customer 360 Audiences for the "Americas & APAC" region as described in the Infrastructure and Sub-processors Documentation:
    - **ASIP Santé certification:** Salesforce has obtained the French health data hosting certification (ASIP Santé certification) that enables Salesforce to host French health data for Customer 360 Audiences. Salesforce's most recent ASIP Santé certification is available upon request from your organization's Salesforce account executive.
    - **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for Customer 360 Audiences 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 Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's Salesforce account executive.

- **NEN-7510**: NEN7510 provides specific controls supplementary to ISO27001 applicable to the Dutch healthcare sector and organizations processing Dutch healthcare data. Salesforce has engaged an independent third-party assessor to map the relevant NEN7510 controls against Salesforce's existing certifications and controls. Salesforce's most recent NEN-7510 report is available for download on Salesforce's compliance website.
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to Customer 360 Audiences undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 or SOC 3 audits. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 reports are available for download on Salesforce's compliance website.

ADVERTISING STUDIO

- Notwithstanding anything to the contrary contained herein, the Salesforce Security Guide is not applicable to Advertising Studio. For additional information on the security controls and user authentication for Advertising Studio, please see the Security Controls and User Authentication sections in the Marketing Cloud Security, Privacy and Architecture Documentation.
- Notwithstanding anything to the contrary contained herein, the "Setup Audit Trail" (which allows customers to view and download certain administrative changes to the Covered Services) as described in the Security Policies and Procedures section above is not applicable to Advertising Studio.
- After termination of the Advertising Studio[7] services, following the 30-day period for return of Customer Data, Customer Data submitted to such services is retained in inactive status for up to 90 days, after which it is securely overwritten or deleted. For the Advertising Studio services, back-up data may be retained for an additional 90 days after deletion of Customer Data, after which it is securely overwritten or deleted.

[7] In the case of Advertising Studio services which are not terminated at the same time as ExactTarget services are terminated, customers may request deletion of Customer Data submitted to the Advertising Studio services by contacting marketingcloudsupport@salesforce.com.