Security, Privacy and Architecture of the Salesforce Marketing Cloud

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 Salesforce Marketing Cloud services (collectively, for the purposes of this document, the "Covered Services"):

- **Advertising Studio**: Services branded or sold as Advertising Studio, Advertising Audiences, or Journey Builder Advertising.
- **Datorama**: Services branded or sold as Datorama.
- **Datorama Reports for Marketing Cloud:** Services branded or sold as Datorama Reports for Marketing Cloud.
- **Evergage**: Services branded or sold as Evergage, Data Science Workbench, or Data Warehouse.
- **ExactTarget**: Services branded or sold as Audience Builder, Automation Studio, Content Builder, Email Studio, Journey Builder, Mobile Studio, or Web Studio.
- **Interaction Studio (Legacy):** Services branded or sold as Interaction Studio.[1].
- **Interaction Studio**: Services branded or sold as Interaction Studio.[2]
- **Marketing Cloud Einstein**: Services branded or sold as Behavioral Triggers, Einstein Content Tagging, Einstein Copy Insights, Einstein Email Recommendations, Einstein Engagement Frequency, Einstein Engagement Scoring for Email (formerly branded as Predictive Scoring), Einstein Engagement Scoring for Mobile, Einstein Messaging Insights, Einstein Recommendations, Einstein Send Time Optimization for Marketing Cloud, Einstein Send Time Optimization for Pardot Einstein Content Selection, Einstein Web Recommendations, Live Weather Block, Personalization Builder, Predictive Email, Predictive Intelligence, Predictive Web, Web & Mobile Analytics, and Web Personalization.
- **Social Studio**: Services branded or sold as Social Studio.

This documentation does not apply to services branded as Audience Studio (formerly branded as Salesforce DMP) and Salesforce Data Studio (together, formerly branded as Krux), or Pardot.

Services Accessed Through, and/or Provided Using Infrastructure Used By, Other Services

Customers may access and use a Service listed below (a "Listed Service") through another Service (an "Underlying Service") described in this or a separate Trust and Compliance Documentation

[1] Applicable to customers purchasing or renewing subscriptions to Interaction Studio (Legacy) on or after October 18, 2018. Customers purchasing Interaction Studio prior to October 18, 2018 purchased Interaction Studio as a Non-Salesforce Application subject to the Terms of Use of Thunderhead (One) Ltd.) For clarity, subscriptions of "Interaction Studio" purchased pursuant to a SFDC Order Form prior to August 18, 2020 shall mean Interaction Studio (Legacy).

[2] Applicable to customers purchasing or renewing subscriptions of Interaction Studio hosted by Amazon Web Services, Inc. as indicated in the Infrastructure and Sub-processors for the Salesforce Marketing Cloud Services documentation here.

("Documentation"). This Documentation describes the back-end infrastructure used by an Underlying Service to store and process Customer Data for the Listed Service. The Underlying Service, including any data stored on the Underlying Service, any predictions written back to the Underlying Service, any functionality and integration presented back to the Underlying Service, and User's login to the Underlying Service, remains subject to the sections of this Documentation applicable to the Underlying Service. Additionally, portions of the Listed Services are provided using technology infrastructure ("Underlying Infrastructure") used by the Services described in the Documentation referenced in the table below.

Listed Services	Underlying Service	Underlying Infrastructure Documentation
Advertising Studio	ExactTarget Services	Marketing Cloud Documentation, specifically those terms that apply to ExactTarget
Datorama Reports for Marketing Cloud	ExactTarget Services, to the extent Customer accesses through ExactTarget; and Datorama Services, to the extent Customer accesses through Datorama	Marketing Cloud Documentation, specifically those terms that apply to Datorama Einstein Platform Documentation
Einstein Vision for Social Studio	N/A	Einstein Platform Documentation
Behavioral Triggers, Einstein Content Selection, Einstein Content Tagging, Einstein Email Recommendations, Einstein Engagement Frequency, Einstein Engagement Scoring for Mobile, Einstein Messaging Insights, Einstein Recommendations, Einstein Send Time Optimization for Marketing Cloud, Einstein Web Recommendations, Live Weather Block, Personalization Builder, Predictive Email, Predictive Intelligence, Predictive Web, Web & Mobile Analytics, and Web	ExactTarget Services	Marketing Cloud Documentation, specifically those terms that apply to ExactTarget

Personalization		
Einstein Send Time Optimization for Pardot	Pardot	Pardot Documentation
Einstein Engagement Scoring for Email (formerly branded as Predictive Scoring) and Einstein Copy Insights	ExactTarget Services; Einstein Platform	Marketing Cloud Documentation, specifically those terms that apply to ExactTarget Einstein Platform Documentation
Interaction Studio (Legacy)	N/A	Heroku 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 customer-specific unique identifiers 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 Covered Services.

Third-Party Functionality

When customers use the ExactTarget Services 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, and (b) carriers – entities that provide wireless messaging services to subscribers via wireless telecommunication networks. These aggregators and carriers may access, store, and transmit message content and related information to provide these functions.

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**[3]: Customer Data submitted to the Advertising Studio, Datorama, ExactTarget, Marketing Cloud Einstein, and Social Studio is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks 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" for Advertising Studio, Datorama, ExactTarget, Marketing Cloud Einstein, and Social Studio.
- **ISO 27001/27017/27018 certification:** Salesforce operates an information security management system (ISMS) for Advertising Studio, Datorama, ExactTarget, Marketing Cloud Einstein, and Social Studio 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.
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to Advertising Studio, Datorama, ExactTarget, Interaction Studio, Marketing Cloud Einstein, and Social Studio undergoes an independent evaluation in the form of a SOC 2 report. Salesforce's most recent SOC 2 reports are available upon request from your organization's Salesforce account executive.
- **TRUSTe certification**: Salesforce's Website Privacy Statement and privacy practices related to Advertising Studio, ExactTarget, Marketing Cloud Einstein and Social Studio 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.
- **HITRUST certification:** For the ExactTarget services, Salesforce has obtained HITRUST CSF Certification. A copy of Salesforce's HITRUST letter of certification is available upon request from your organization's Salesforce Account Executive.
- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Advertising Studio, Datorama, Datorama Reports for Marketing Cloud, ExactTarget, Marketing Cloud Einstein, and Social Studio 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/.
- **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/.

Additionally, 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.

As further described in the "Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by third parties to host Customer Data submitted to certain services. Specifically,

[3] Services that are made generally available after July 16, 2020 will no longer be added to Salesforce's Privacy Shield Certification, including: Datorama Reports for Marketing Cloud.

Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host Customer Data submitted to Datorama, Datorama Reports for Marketing Cloud, Interaction Studio and Evergage, and Marketing Cloud Einstein. Salesforce uses infrastructure provided by Google, LLC ("GCP") to host Customer Data submitted to ExactTarget. Salesforce uses infrastructure provided by Microsoft Corporation ("Azure") to host Customer Data submitted to Datorama, Datorama Reports for Marketing Cloud and Interaction Studio (Legacy). Information about security and privacy-related audits and certifications received by AWS, GCP, and Azure, including ISO 27001 certification and SOC reports, is available from the AWS Security website, the AWS Compliance website, the Google Security website, the Google Compliance website, the Azure Security website, and the Azure Compliance website.

Security Controls

The Covered Services include a variety of security controls. These controls include:

- Unique user identifiers allow customers to assign unique credentials for their users and assign and manage associated permissions and entitlements.
- Controls to ensure initial passwords must be reset on first use.
- Controls to limit password re-use.
- Password length and complexity requirements.
- Customers have the option to vary the complexity, expiration, and challenge questions regarding password security, and to define additional security settings such as account lockout in ExactTarget, Advertising Studio, Datorama Reports for Marketing Cloud and Marketing Cloud Einstein.
- Customers of Advertising Studio, Datorama, Datorama Reports for Marketing Cloud, ExactTarget, Interaction Studio (Legacy), Marketing Cloud Einstein, and Social Studio have the option to define the range of IP addresses from which their users may access the Covered Services.
- Encryption and decryption options for data used to construct email messages and landing pages in ExactTarget.
- Email export allowlist functionality enables customers to define which users are able to receive exported material via email from ExactTarget, Evergage, and Interaction Studio.
- Customers have the option to manage their application users, and assign or define roles, or apply permissions and rights, within their implementation of the Covered Services.
- Where SFTP or FTP uploads are available within the Covered Services, Customers have the ability to use their own external SFTP or FTP accounts to upload customer content to the Covered Services. If a customer desires that Salesforce provide an inbound SFTP account to the customer, the customer sets its own password for that account. Customers of Advertising Studio, ExactTarget, Marketing Cloud Einstein, and Social Studio may also request Login IP Allowlisting for a Salesforce-provisioned SFTP account by contacting their support representative. Inbound SFTP accounts are otherwise not subject to the security controls, procedures, or policies in this document.
- Multi-Factor Authentication and Single Sign-On for access to the Covered Services as set forth in the applicable Notices and License Information (NLI).

Some Covered Services use AWS, GCP, or Azure, as described above; further information about security provided by AWS, GCP, and Azure is available from the AWS Security website, including AWS's overview of security processes, the Google Security website, the Google Compliance website, and the Azure Security website.

Security Policies and Procedures

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

- User passwords are stored using a salted hash format and are not transmitted unencrypted.
- Social account OAuth tokens used within Social Studio are encrypted with a minimum of 128-bit AES encryption.
- User access log entries will be maintained, containing date, time, URL executed or identity ID operated on, operation performed (accessed, created, edited, deleted, etc.) and source IP address.
- If there is suspicion of inappropriate access to the Covered Services, Salesforce can provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- User access logs will be stored in a secure centralized host to prevent tampering.
- User access logs will be kept for a minimum of 90 days.
- Salesforce personnel will not set a defined password for a user.

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the Covered 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 plugins, enabled MIME types, etc.) for security purposes, including 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, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (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 user ID and password combination, which are encrypted via TLS while in transmission, as well as machine specific information for identity validation as described under "Security Controls," above. 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 guards, two-factor access screening, and escort-controlled access, and are also supported by on-site backup generators in the event of a power failure.

Reliability and Backup

All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Covered Services is stored on infrastructure that supports high availability and is backed up on a regular basis. This backup data for Advertising Studio, ExactTarget, Interaction Studio (Legacy), and Marketing Cloud Einstein is retained for 90 days. Backup data for Datorama and Datorama Reports for Marketing Cloud is retained for 30 days and backup data for Social Studio is retained as needed to provide business continuity. Backup data for Interaction Studio and Evergage is retained as needed to provide business continuity, generally for a period of 1-30 days.

Disaster Recovery

The Covered Services' production systems are protected by disaster recovery plans which provide 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 an outage.

Datorama, Datorama Reports for Marketing Cloud, ExactTarget, Evergage, Interaction Studio (Legacy), Interaction Studio, Marketing Cloud Einstein, and Social Studio use secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and internet connectivity, in the event production facilities at the primary data centers were to be rendered unavailable.

Viruses

The Covered Services have controls in place that are designed to prevent the introduction of viruses to these Services' respective platforms. Uploaded attachments that are found to contain a virus will not be executed in ExactTarget and will not be stored in Social Studio and Interaction Studio (Legacy). Uploaded attachments are not executable in Advertising Studio, Datorama, Datorama Reports for Marketing Cloud, Evergage, Interaction Studio (Legacy), Interaction Studio, Marketing Cloud Einstein, and Social Studio and therefore will not damage or compromise the online Advertising Studio, Datorama, Datorama Reports for Marketing Cloud, Evergage, Interaction Studio (Legacy), Interaction Studio, Marketing Cloud Einstein, and Social Studio services by virtue of containing a virus. Additionally, Social Studio may pull in information from the Internet and links to other websites that may contain malicious content, but such websites are not executable in Social Studio.

Data Encryption

The Covered Services use, or enable customers to 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) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum.

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. Within 30 days of termination of the applicable Covered Service, customers may 1) request return of Customer Data submitted to Advertising Studio, Interaction Studio (Legacy), or Social Studio by contacting marketingcloudsupport@salesforce.com; 2) access their account to export or download Customer Data submitted to ExactTarget; or 3) contact their account manager to download or export reports generated by the Marketing Cloud Einstein features branded as Einstein Email Recommendations or Einstein Web Recommendations, Datorama Reports for Marketing Cloud or Datorama or Customer Data submitted to Interaction Studio, or Evergage and engage Salesforce

professional services to recover any raw data processed by the Marketing Cloud Einstein features branded as Einstein Email Recommendations or Einstein Web Recommendations that has not already been deleted.

Deletion of Customer Data

After termination of the Advertising Studio[4], Evergage, ExactTarget, Datorama Reports for Marketing Cloud, Interaction Studio (Legacy), Interaction Studio, or Marketing Cloud Einstein 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. After termination of the Datorama or Social Studio services, following the 30-day period for return of Customer Data, Customer Data submitted to Datorama or Social Studio is retained in inactive status for up to 60 days, after which it is securely overwritten or deleted. For all Covered 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.

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 Salesforce Marketing Cloud 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 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).

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 or any Covered Service 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 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.

[4] 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.

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.

Additionally, Salesforce uses Customer Data consisting of data and metrics derived from customer's websites and social accounts with third-party social platforms, such as geographic location, time of day of use, greatest period of use by industry, and other metrics including spend rates or click rates by geographic location and by industry to create an aggregated and anonymized data set ("Anonymized Data"). No Customer Data consisting of personally identifiable information is contained in the Anonymized Data, nor any data that would identify customers, their users, customers' clients, or any individual, company or organization. Salesforce combines the Anonymized Data with that of other customers to create marketing reports and to provide product features. By using the Covered Services, customers consent to the use and disclosure of their Customer Data to create reports from the Anonymized Data.

Interoperation with Other Services

The Covered Services may interoperate or integrate with one another, and with other services provided by Salesforce or third parties. Security, Privacy and Architecture documentation for such 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.