Einstein Platform Security, Privacy and Architecture
Published: January 17, 2020

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 and information obtained by SFDC from publicly available sources or its third party content providers and made available to Customer through the Services, Beta Services or pursuant to an Order Form (“Content”).

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 follows (collectively, for the purposes of this document, the “Covered Services”):

- Sales Cloud Einstein
- Pardot Einstein
- Salesforce Inbox
- High Velocity Sales
- Einstein Engagement Scoring
- Einstein Vision and Language
- Einstein Bots
- Einstein Prediction Builder (included in Einstein Analytics Plus and Einstein Prediction)
- Service Cloud Einstein
- Einstein Vision for Social Studios

This document also applies to a Customer’s use of

- Einstein Activity Capture feature and Einstein Opportunity Scoring feature as part of the Sales Cloud Service
- Einstein Bots feature, Einstein Case Classification feature, and Einstein Article Recommendations feature as part of the Service Cloud Service
- Einstein Object Detection feature as part of the Consumer Goods Cloud Service
- Einstein Prediction Builder feature as part of Sales Cloud, Service Cloud, or Lightning Platform.

This documentation does not apply to Einstein-branded services or features unless listed above.

Covered Services Accessed through other Salesforce Services
To the extent a Covered Service is accessed through 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. For example, Customer’s use of Sales Cloud Einstein contemplates that the service may copy, store, and process Customer Data from Sales Cloud, and Sales Cloud Einstein will

1 Rights of ALBERT EINSTEIN are used with permission of The Hebrew University of Jerusalem. Represented exclusively by Greenlight.
provide relevant scores and predictions to enrich Customer’s Sales Cloud data which are displayed and stored in Sales Cloud. With the exception of Einstein Vision and Language, the Covered Services covered by this Security, Privacy and Architecture Documentation remain subject to other documentation as follows:

<table>
<thead>
<tr>
<th>Covered Service</th>
<th>Additional Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Cloud Einstein</td>
<td>Salesforce Services Documentation, specifically those terms that apply to Sales Cloud and Einstein Analytics</td>
</tr>
<tr>
<td>Pardot Einstein</td>
<td>Pardot Services Documentation</td>
</tr>
<tr>
<td>Salesforce Inbox</td>
<td>Salesforce Services Documentation, specifically those terms that apply to Sales Cloud</td>
</tr>
<tr>
<td>High Velocity Sales</td>
<td>Salesforce Services Documentation, specifically those terms that apply to Sales Cloud</td>
</tr>
<tr>
<td>Einstein Engagement Scoring</td>
<td>Marketing Cloud Documentation, specifically those terms that apply to “ExactTarget” and “Predictive Intelligence”</td>
</tr>
<tr>
<td>Einstein Vision and Language</td>
<td>N/A</td>
</tr>
<tr>
<td>Einstein Bots</td>
<td>Salesforce Services Documentation, specifically those terms that apply to Service Cloud</td>
</tr>
<tr>
<td>Service Cloud Einstein</td>
<td>Messaging Documentation (Einstein Bots only)</td>
</tr>
<tr>
<td>Einstein Prediction Builder (included in Einstein</td>
<td>Salesforce Services Documentation</td>
</tr>
<tr>
<td>Analytics Plus and Einstein Prediction)</td>
<td></td>
</tr>
<tr>
<td>Einstein Vision for Social Studios</td>
<td>Social Studios Documentation</td>
</tr>
</tbody>
</table>

**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. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. Further, except for Einstein Vision and Language, the architecture allows the use of customer and user role based access privileges.

The specific infrastructure used to host Customer Data is described in the “Infrastructure and Sub-processors” documentation for the Covered Services is 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 describes the sub-processors and certain other entities material to Salesforce’s provision of the Covered Services. As described in this documentation, Amazon Web Services, Inc. (“AWS”) provides architecture that supports the provision of the Covered 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 security- and privacy-related audits and certifications are applicable to one or more of the Covered Services, as described below:

- **Binding Corporate Rules (BCR) for Processors**: Customer Data submitted to the Covered Services—with the exception of Einstein Vision for Social Studios, Sales Cloud Einstein, and Service Cloud Einstein—is within the scope of the Salesforce BCR for Processors. The most current version of the Salesforce BCR for Processors is available on Salesforce’s website, currently located at [https://www.salesforce.com/company/privacy/](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 exception of Einstein Vision for Social Studios—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](https://www.privacyshield.gov/list) by searching under “Salesforce.”

- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for Salesforce Inbox, Einstein Activity Capture, and Einstein Prediction Builder 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 Salesforce Inbox is available [here](https://www.salesforce.com/company/privacy/).

- **Service Organization Control (SOC) reports**: Salesforce’s information security control environment applicable to Einstein Prediction Builder and Einstein Case Classification (a feature in Service Cloud Einstein) undergoes an independent evaluation in the form of SOC 1 (SSAE 18/ISAE 3402) and SOC 2.. Salesforce’s most recent SOC 1 (SSAE 18/ISAE 3402) and SOC 2 reports are available upon request from your organization’s Salesforce account executive.

- **TRUSTe certification**: Salesforce’s [Website Privacy Statement](https://www.salesforce.com/company/privacy/) and privacy practices related to the Covered Services—with the exception of Einstein Vision for Social Studios—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](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](http://cbprs.org/compliance).
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 Web site and the AWS Compliance Web site.

Security Controls
With the exception of Einstein Vision and Language, the Covered Services covered by this Security, Privacy and Architecture Documentation remain subject to other documentation as set forth in the chart above.

Security Policies and Procedures
Access to Einstein Vision and Language is via API, and requires a valid API key/secret/token which is encrypted via TLS while in transmission. Einstein Vision and Language are operated in accordance with the following procedures to enhance security:

- Org IDs are assigned to ensure that activities can be attributed to the responsible account.
- Einstein Vision and Language does not use any Customer-defined username or password, authentication is key-based; and
- User access log entries will be maintained, containing date, time, and partial URL.

With the exception of Einstein Vision and Language, which is accessed via the Einstein.ai API, the only User or Administrator access to each of the Covered Services is pursuant to another Service. Accordingly, each such Covered Service remains subject to other documentation as set forth in the “Covered Services Accessed through other Salesforce Services” section above.

Further information about security provided by AWS is available from the AWS Security Website, including AWS’s overview of security processes.

Intrusion Detection
For Salesforce Inbox (including the Einstein Activity Capture component), Salesforce, or an authorized independent third party, will monitor Salesforce Inbox for unauthorized intrusions using multiple 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 prevent fraudulent authentications, and to ensure that Salesforce Inbox functions 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.
User Authentication
Access to Einstein Vision and Language via an API requires an API key/secret/token, both of which are encrypted via TLS while in transmission.

Customers access Sales Cloud Einstein, Pardot Einstein, Salesforce Inbox, High Velocity Sales Einstein Engagement Scoring, Einstein Bots, Einstein Prediction Builder, Service Cloud Einstein, and Einstein Vision for Social Studios through other Salesforce services. For information about user authentication for Einstein Engagement Scoring, please see the Marketing Cloud Security, Privacy, and Architecture documentation available here. For information about user authentication for Sales Cloud Einstein, Salesforce Inbox, High Velocity Sales, Einstein Bots, Einstein Prediction Builder, and Service Cloud Einstein, please see the Salesforce Services Security, Privacy, and Architecture documentation available here. For information about user authentication for Pardot Einstein, please see the Pardot Security, Privacy, and Architecture Documentation available here.

Physical Security
Production data centers used to provide the Covered Services have systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, physical 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, load balancers, Web servers and application servers are configured in a redundant configuration. All 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 daily.

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 within a brief period time.

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.

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 through Transport Layer Encryption (TLS).

Return of Customer Data
During the contract term, customers may export a copy of any Customer Data made available for export through the Covered Services. Within 30 days post contract termination, customers may request return of their respective Customer Data, to the extent such Customer Data can be copied and exported from the
Covered Services and the ability to export such data is generally made available to customers, by contacting their account representative. For the Covered Services, insights, reports, and scoring may be available for manual export only. Salesforce Inbox and Einstein Activity Capture does not support the export of Customer’s activity data or insights generated on this activity data. For Einstein Engagement Scoring, modeling factors are available for manual export only.

Customer Data is not made available for export through Einstein Vision and Language, however customers may delete an entire data set submitted as Customer Data in their use of the services.

**Deletion of Customer Data**

After termination of all subscriptions associated with any of the Covered Services, 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. This process is subject to applicable legal requirements. When a Customer terminates a paid subscription to Einstein Vision and Language, the Customer’s subscription will continue under the free usage tier for Einstein Vision and Language, and the Customer's Data will not be deleted until the Customer terminates their subscription to Einstein Vision and Language entirely.

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**

**Important:** The following types of sensitive personal data (including images, sounds or other information containing or revealing such sensitive 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); racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, information concerning health or sex life; information related to an individual’s physical or mental health; and information related to the provision or payment of health care.

Customer shall not use Einstein Vision, Einstein Language, or Einstein Prediction Builder 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. Additionally, for Einstein Vision, Customer may not submit images of individuals for the purposes of creating or analyzing biometric identifiers, such as face prints or fingerprints or scans of eyes, hands or facial geometry.

If Customer chooses to use any of the Covered Services 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 take account of other factors beyond the Covered Services’ 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 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.

In addition, 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. No Customer Data consisting of personally identifiable information will be shared in this manner, nor any data that would identify customers, their users, their consumers, or any individual, company or organization. By using the Covered Services, customers consent to the use and disclosure of their Customer Data in anonymized and aggregated form.

**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 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.