Hyperforce Security, Privacy and Architecture

Security, Privacy and Architecture of Salesforce services and features[1]
Published: November 21, 2025

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 MSA.

Services and Features 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 as operating on Hyperforce (formerly Salesforce Unified Cloud) (collectively, for the purposes of this document only, the "Covered Services"):
   (1) the services and features branded as:
   - Accounting Subledger,
   - Archive, a feature of Lightning Platform (including Force.com),
   - Automotive Cloud[2] [8]
   - B2B Commerce on Lightning Experience[3]
   - B2C Commerce/Commerce Cloud[4]
   - Chatter
   - Communications Cloud[5]
   - Configuration Management Database (CMDB), a component of Agentforce IT Service
   - Consumer Goods Cloud (including Trade Promotion Management, Trade Promotion Optimization, and Retail Execution)[8]
   - Salesforce Data 360(aka Customer Data Cloud)
       - Customer Data Platform (formerly branded as Salesforce CDP)
   - Database.com
   - Education Cloud
   - Einstein Relationship Insights[6]
   - Einstein Personalization
   - Employee Service[7]
   - Energy & Utilities Cloud[4]

---

[1] For the full list, please refer to "Services and Features Covered"

[2] This documentation applies to Digital Lending for Automotive Cloud.

[3] B2B Commerce on Lightning Experience refers to the version provisioned on or after July 20, 2020. B2B Commerce refers to the managed package version 3.97 (Release 3.8) or higher.

[4] [B2C Commerce or Salesforce Commerce Cloud ("Demandware"), which includes Commerce Cloud Digital (B2C Commerce GMV or B2C Commerce PPO) (collectively, the "B2C Commerce Services"), provided by Salesforce, Inc., Demandware, LLC a Salesforce, Inc. company.]

[5] Some purchases of Communications Cloud, Financial Services Cloud, Health Cloud, Life Sciences Cloud, Media Cloud, and Energy & Utilities Cloud services may include a license for Vlocity Services.

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

[7] Employee Service includes the following Einstein features: Article Recommendations, Case Wrap-Up, and Case Classification, which are subject to the Einstein Platform Documentation as stated below.

- Enablement (including Enablement Lite)
- Enhanced Messaging
- Experience Cloud (formerly Community Cloud)
- Feedback Management (formerly Salesforce Surveys)
- Flow for Industries (formerly Digital Process Automation) (including Server-Side Document Generation)
- Lightning Platform (including Force.com, but excluding those provided for free as noted in (8) in the next section below)
- Marketing Cloud Engagement (formerly ExactTarget)
- Marketing Cloud Einstein
- Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition (including Mobile App Messaging)
- Marketing Intelligence
- Headless Browser Service
- Intelligent Form Reader
- Loyalty Management
- Manufacturing Cloud
- Media Cloud[4]
- Messaging
- Enhanced Chat (formerly Messaging for In-App and Web)
- Microsoft Teams Integration
- MuleSoft[8]
- Nonprofit Cloud,
- Nonprofit Cloud Case Management[9],
- Nonprofit Cloud for Grantmaking,
- Process Compliance Navigator,
- Public Sector Solutions[10]
- Retail Cloud POS
- Referral Marketing
- Revenue Cloud[11]
- Revenue Cloud Billing
- Sales Cloud[8]
- Salesforce Order Management[12]
- Salesforce Private Connect
- Salesforce Sales Planning

---

[8] MuleSoft includes the MuleSoft Anypoint Platform. MuleSoft also includes features that may use the Einstein Generative AI Services; please see the [infrastructure details](#) for these features

[9] References to Nonprofit Cloud Case Management refer to the managed package.

[10] Some purchases of Public Sector Solutions may include a license for Emergency Program Management, Vlocity Services, Employee Productivity, or a combination of the foregoing licenses. Emergency Program Management and Employee Productivity are included in this documentation.

[11] "Revenue Cloud" includes the SKUs branded as "Revenue Cloud Growth" and "Revenue Cloud Advanced." Revenue Cloud Advanced (formerly Revenue Lifecycle Management) includes access to Salesforce Contracts, Document Builder, and product and quoteline functionality.

[12] Any reference to Salesforce Order Management in this Documentation describes the Security, Privacy and Architecture of the version of Order Management released on February 19, 2020 ("Salesforce Order Management"). For versions of Order Management released prior to the release of Salesforce Order Management ("B2C Commerce Order Management"), such versions shall continue to be governed by the B2C Commerce Documentation.

- Salesforce Shield[13]
- Salesforce Slack Integration Proxy
- Salesforce Spiff (US-based instances provisioned or migrated on or after January 30, 2025; EU-based instances provisioned or migrated on or after February 18, 2025)
- Service Cloud
- Service Cloud Voice
- Site.com
- Tableau Cloud
- CRM Analytics[14]
- WDC[15]
- Workforce Engagement Management
- MC Advertising
- B2B Commerce[5]
- Emergency Program Management
- Employee Productivity
- Salesforce Field Service managed package ("FSMP"), which is a feature of Service Cloud. FSMP customers have access to optional scheduling optimization functionalities including the "FS Optimizer", "Enhanced Scheduling and Optimization", and "Work Bundling" and optional document and PDF generation functionality through "Document Builder".
- Financial Services Cloud (including Digital Lending)[4]
- Health Cloud[4]
- Life Sciences Cloud[4]
- Net Zero Cloud (formerly Sustainability Cloud)
- Privacy Center
- Salesforce Contracts
- Salesforce CPQ and Salesforce Billing (together formerly branded as Salesforce Quote-to-Cash)
- Salesforce Maps (including Maps Lite)
- Shift Management
- Subscription Management
- Unified Messaging
- Vlocity managed packages and features ("Vlocity Services") branded as:
  - Vlocity Communication package
  - Vlocity Media and Entertainment package,
  - Vlocity Energy & Utilities package,
  - Vlocity Insurance package,
  - Vlocity Health package,
  - Vlocity Public Sector or Vlocity Government package,
  - Vlocity Digital Commerce Gateway,
  - Vlocity Order Management Plus,
- Marketing in Salesforce Starter, including Marketing Email Sends, may be included in Salesforce Starter (fka Self-Service CRM), ProSuite, and CRM Foundations[16]

---

[13] Salesforce Shield includes Data Detect, Event Monitoring, Field Audit Trail, and Platform Encryption (which includes the Encryption Key Management and Tenant-Level Encryption features).

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

[15] WDC refers to Services formerly branded as Work.com provisioned before May 1, 2020

[16] Marketing in Salesforce Starter, ProSuite, and CRM Foundations including Marketing Email Sends includes features

(2) the Salesforce.org, LLC ("Salesforce.org") services and features branded as:
- Admissions Connect,
- foundationConnect[17],
- Grants Management,
- Salesforce.org Insights Platform: Data Integrity ("Insights Platform"), and
- Student Success Hub (including the former Salesforce Advisor Link).

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, designated as on the Hyperforce Operating Zone (formerly EU Operating Zone) infrastructure, or is sold on a SKU that includes "HF OZ" in the SKU name.

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." Scratch Orgs are for testing and development use only, and not for production use, and should not contain personal data.
(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) Certain Einstein products and features run on multiple infrastructures. When using any of these products and features independently or in conjunction with the Covered Services, as applicable, this Documentation and Einstein Platform Documentation[18] applies: Account Intelligence, Marketing Intelligence, Agentforce Voice, Einstein Activity Capture, Einstein Article Recommendations, Einstein Bots, Einstein Case Classification, Einstein Case Wrap-up, Einstein Conversation Insights, Einstein Deal Insights, Einstein for Sales, Einstein for Service, Einstein for Platform, Einstein GPT for Sales, Einstein GPT for Service, Einstein Object Detection, Einstein Opportunity Scoring, Einstein Prediction Builder,[19] Einstein Recommendation Builder, Enablement (not including Enablement Lite), Sales Engagement (formerly High Velocity Sales), Sales Cloud Einstein, Salesforce Inbox, Service Cloud Einstein, Workforce Engagement Management (if the Intelligent Forecasting Machine Learning feature is enabled); and Einstein Personalization.

---

of Salesforce Data 360(aka Customer Data Cloud), Experience Cloud, Lightning Platform, Marketing Cloud Engagement (formerly ExactTarget), Marketing Cloud Einstein, Sales Cloud, Service Cloud, and Privacy Center. Marketing in Salesforce Starter, ProSuite, and CRM Foundations is included in this documentation and is also subject to the Salesforce Services, Marketing Cloud, Salesforce Data 360(aka Customer Data Cloud) and Marketing Cloud Account Engagement (formerly Pardot) Documentation.

[17] This documentation only applies to foundationConnect provisioned on or after August 19, 2019.

[18] Certain Covered Services offered for Salesforce Industries Clouds utilize integrations with Einstein Generative AI Services. These Einstein Generative AI Services: (i) employ OpenAI's generative AI models; and (ii) employ Azure OpenAI generative AI models through Microsoft, in each case to provide the Services, as described further in the Einstein Platform Documentation.

[19] Einstein Prediction Builder is included in several CRM Analytics SKUs, including Einstein Predictions, and CRM Analytics Plus and related SKUs. Additionally, certain CRM Analytics SKUs that are branded "Intelligence", such as Manufacturing Cloud Intelligence, include certain features of Sales Cloud Einstein as well as Einstein Prediction Builder. The CRM Analytics Services run on infrastructure described by this Documentation, and the Einstein Prediction Builder Service and Sales Cloud Einstein features run across infrastructure described in this Documentation

(4) Customers may choose to use related products and features branded as Quip[20]; these features run across two infrastructures, the infrastructure described by this Documentation, and the infrastructure described by the 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, Commerce Cloud Einstein (including services branded by Demandware, Inc. as Predicative Email), LiveMessage, and Marketing Cloud. Among such services are the CRM Analytics Plus and Einstein Prediction Services which contain features that run on different infrastructures: the CRM Analytics Services runs on infrastructure described by this Documentation, and the Einstein Prediction Builder Service runs across infrastructure described by the Einstein Platform Documentation.

(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](#).

(8) Lightning Platform Developer Edition and its associated products and services that are provided for free.

(9) The MC Advertising services are accessed through the Marketing Cloud Engagement 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 Marketing Cloud Engagement services.

(10) Heroku Documentation for Salesforce Functions, Student Success Hub and Insights Platform.

(11) Certain Referral Marketing products and features run on multiple infrastructures: When using any of these products and features independently or in conjunction with the Covered Services, as applicable, this Documentation and the Marketing Cloud Documentation applies.

(12) Certain Tableau Cloud services and features may run on the infrastructure described in the "Infrastructure and Sub-processors" documentation available [here](#).

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 Vlocity Digital Commerce Gateway services and Vlocity Order Management Plus service, are operated in an architecture providing logical data separation for different customers via customer-specific accounts. 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 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.

---

[20] Quip includes Services formerly branded as Salesforce Anywhere.

The "Infrastructure and Sub-processors" documentation available 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. Except as specified below, Salesforce's most recent audit reports and certifications are available for download at Salesforce's compliance website.

- **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/.
- **Hébergeur de Données de Santé (HDS):** Salesforce has obtained the French health data hosting certification (HDS certification) that enables Salesforce to host French health data. The HDS certification names the Covered Services with the following exceptions: (i) Accounting Subledger, Agentforce IT Service, B2C Commerce, Consumer Goods Cloud, Feedback Management, Employee Service, Education Cloud, Einstein Relationship Insights, Messaging, Process Compliance Navigator, Salesforce Maps, Salesforce Sales Planning, Microsoft Teams Integration, Nonprofit Cloud, Nonprofit Cloud for Grantmaking, Insights Platform, Workforce Engagement Management, Intelligent Form Reader, Privacy Center, , Shift Management, Student Success Hub, Encryption Key Management, Tenant-Level Encryption, Marketing in Salesforce Starter, Enablement, Insurance Brokerage, and Referral Marketing (collectively the "**Certification Excluded Services**"); (ii) Emergency Program Management; (iii) Digital Lending; (iv) WDC; (v) Communications Cloud, Energy & Utilities Cloud, Media Cloud, and Vlocity Services; (vi) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition, (vii) Admissions Connect; (viii) Automotive Cloud; (ix) Education Cloud; (x) Salesforce Contracts; (xi) Einstein Personalization; (xii) Salesforce Spiff; (xiv) Revenue Cloud; (xv) Retail Cloud POS; and (xvi) Revenue Cloud Billing.
- **Cloud Computing Compliance Criteria Catalogue (C5).** Salesforce has obtained Cloud Computing Compliance Criteria Catalogue (C5). The C5 certification names the Covered Services with the following exceptions: the (i) Certification Excluded Services; (ii) MC Advertising; (iii) B2C

Commerce, (iv) Customer Salesforce Data 360; (v) Digital Lending; (vi) FSMP, including FS Optimizer, Enhanced Scheduling and Optimization, and Work Bundling; (vii) Marketing Cloud Engagement; (viii) Marketing Cloud Einstein, (ix) Communications Cloud, Energy & Utilities Cloud, Media Cloud, and Vlocity Services; (x) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition; (xi) Tableau Cloud; (xii) Einstein Personalization; (xiii) Salesforce Spiff; (xiv) Retail Cloud POS; (xv) Revenue Cloud Billing; (xvi) MuleSoft; (xvii) Marketing Intelligence, and (xviii) Agentforce IT Service.

- **Esquema Nacionale de Seguridad (ENS):** Salesforce has obtained (Esquema Nacional de Seguridad) ENS certification at ENS High. The ENS certification names the Covered Services with the following exceptions: the (i) Certification Excluded Services; (iii) foundationConnect; (iv) Salesforce Data 360; (v) Digital Lending; (vi); (vii) Service Cloud Voice; (viii) WDC; (x) FSMP, including FS Optimizer, Enhanced Scheduling and Optimization, and Work Bundling; (xi) Marketing Cloud Engagement; (xii) Marketing Cloud Einstein,(xiii); (xiv); (xv) Communications Cloud, Energy & Utilities Cloud, Media Cloud, and Vlocity Services; (xvi) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition; (xvii) Flow for Industries; (xviii) Education Cloud; (xx) Life Sciences Cloud; (xxi) Tableau Cloud; (xxii) Einstein Personalization; (xxiii) Salesforce Spiff; (xxiv) Revenue Cloud; (xxv) Retail Cloud POS;(xxvi) Revenue Cloud Billing; (xxvii) MuleSoft, and (xix) Agentforce IT Service.
- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Covered Services is within the scope of the Salesforce EU and UK BCR for Processors to the extent described therein.
- **Data Privacy Framework Certifications:** Customer Data submitted to the Covered Services is within the scope of annual certifications to the EU-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, and Swiss-US Data Privacy Framework as administered by the US Department of Commerce and further described in our [Notice of Certification](). The current certifications are available at https://www.dataprivacyframework.gov/s/ by searching under "Salesforce."
- **HITRUST:** HITRUST safeguards sensitive information and manages information risk for organizations in the healthcare industry and throughout the third-party supply chain. The HITRUST certification names specific regions and the Covered Services with the following exceptions: the (i) Certification Excluded Services; (ii) MC Advertising; (iii) foundationConnect; (iv) Salesforce Data 360; (v) Headless Browser Service; (vi) Salesforce Slack Integration Proxy; (vii) Public Sector Solutions; (viii) FSMP, including FS Optimizer, Enhanced Scheduling and Optimization, and Work Bundling; (ix) Marketing Cloud Engagement; (x) Marketing Cloud Einstein; (xi) Enhanced Messaging); (xii) Enhanced Chat (formerly Messaging for In-App and Web); (xiii) Communications Cloud, Energy & Utilities Cloud, Media Cloud, and Vlocity Services; (xiv) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition; and (xv) Unified Messaging; and (xvi) Automotive Cloud; (xvii) Flow for Industries; and (xviii) Education Cloud. (xix) Nonprofit Cloud for Grantmaking; (xx) Employee Productivity; and (xxi) Salesforce Contracts; (xxii) Salesforce Order Management; and (xxiii) Student Success Hub; (xxiv) Subscription Management; (xxv) Financial Services Cloud; (xxvi) Health Cloud; (xxvii) Manufacturing Cloud; and Salesforce CPQ and Salesforce Billing; Nonprofit Cloud Case Management; and Grants Management; (xxviii) Life Sciences Cloud; (xxix) Digital Lending; (xxx) Tableau Cloud; (xxxi) Einstein Personalization; (xxxii) Salesforce Spiff; (xxxiii) Retail Cloud POS; (xxxiii) Revenue Cloud; (xxxiv) Revenue Cloud Billing; (xxxv) MuleSoft, and (xxxvi) Agentforce IT Service. For more information on the regions where Salesforce has HITRUST certification, please refer to Salesforce's compliance [website]().

- **IRAP Assessment:** Salesforce has obtained an InfoSec Registered Assessor Program (IRAP) Assessment against the Australian Government Information Security Manual up to the PROTECTED level. The IRAP Assessment applies to Services on Hyperforce instances in Australia and names the Covered Services with the following exceptions: (i) the Certification Excluded Services; (ii) MC Advertising; (iii) foundationConnect; (iv) Grants Management; (v) Digital Lending; (vi) Emergency Program Management; (vii) FSMP, including FS Optimizer, Enhanced Scheduling and Optimization, & Work Bundling; (viii) Communications Cloud, Energy & Utilities Cloud, and Media Cloud; (ix) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition; and (x) Unified Messaging; (xi) Admissions Connect; (xii) Automotive Cloud; and (xiii) Education Cloud; and (xiv) Nonprofit Cloud for Grantmaking; (xv) Salesforce Contracts; and (xvi) Student Success Hub; Nonprofit Cloud Case Management; (xvii) Tableau Cloud; (xviii) Einstein Personalization; (xix) Salesforce Spiff; (xx) Retail Cloud POS; (xxi) Revenue Cloud; (xxii) Revenue Cloud Billing; (xxiii) MuleSoft, and (xxiv) Agentforce IT Service.
- **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 ISO certifications name the Covered Services with the following exceptions: (i) the Certification Excluded Services; (ii) Digital Lending; and (iii) Retail Cloud POS, and (iv) Agentforce IT Service. (v) WDC; and (vi) Public Sector Solutions
- **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. The NEN-7510 certification names the Covered Services with the following exceptions: (i) the Certification Excluded Services; (ii) Service Cloud Voice; WDC; Enhanced Messaging (iii) Communications Cloud; (iv) Energy & Utilities Cloud; (v) Media Cloud; (vi) Vlocity Services; (vii) Digital Lending; (viii) Einstein Personalization; (ix) Salesforce Spiff; (x) Retail Cloud POS; (xi) Revenue Cloud, and (xii) Agentforce IT Service.
- **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). The AOC names the Covered Services with the following exceptions: (i) the Certification Excluded Services; (ii) MC Advertising; (iii) foundationConnect; (iv) Grants Management; (v) Salesforce Slack Integration Proxy; (vi) Workplace Command Center; (vii) Salesforce Data 360; (viii) Service Cloud Voice; (ix) WDC; (x) FSMP, including FS Optimizer, Enhanced Scheduling and Optimization, & Work Bundling, (xi) Enhanced Messaging; (xii) Messaging for In-App and Web; (xiii) Marketing Cloud Engagement; and (xiv) Communications Cloud, Energy & Utilities Cloud, Media Cloud, and Vlocity Services; (xv) Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition; (xvi) Unified Messaging, and (xvii) Admissions Connect; (xviii) Nonprofit Cloud; (xix) Nonprofit Cloud for Grantmaking; (xx) Employee Productivity; (xxi) Salesforce Contracts; (xii) Student Success Hub; (xv) Nonprofit Cloud Case Management; (xiii) Life Sciences Cloud; (xiv) Tableau Cloud; (xv) Einstein Personalization; (xvi) Salesforce Spiff; (xvii) Retail Cloud POS; (xviii) Revenue Cloud Billing, and (xix) Agentforce IT Service. As of the date Published, the AOC applies to the applicable Services on Hyperforce instances in Australia, Brazil, Canada, France, Germany, India, Japan, Singapore, and the United States. 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](). Additionally, the Salesforce Field Service Tap-to-Pay feature of the mobile application has been validated to PCI DSS SAQ-D for Service Providers, and more information is available upon request from your organization's Salesforce account executive.

- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to Salesforce services on Hyperforce undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 or SOC 3 audits. The SOC reports names the Covered Services with the exception of the Certification Excluded Services, and Digital Lending.
- **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]().

As further described in the "Infrastructure and Sub-processors" documentation available [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 Website]() 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](), 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 (if stored at all) 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.

9

- 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.[21]

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/

---

[21] This sentence does not apply to Headless Browser Service or Salesforce Slack Integration Proxy, which use a proxy – rather than a session ID – for authentication.

Reliability, Backup, Business Continuity, and Disaster Recovery[22]

Salesforce Unified Cloud (Hyperforce) is configured and deployed in a highly available[23] manner. The systems are designed to recover from failure in a minimally disruptive[24] 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[25], 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 once 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[26] 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.

For the purposes of preventing fraud or abuse and to comply with applicable law, hosting provider AWS reserves the ability to access systems processing and storing encrypted Customer Data. Salesforce has implemented technical measures that prevent AWS from accessing unencrypted Customer Data and from accessing encryption keys used to encrypt Customer Data. With Platform Encryption, Customers may generate and store encryption key material outside of Salesforce.

---

[22] This section does not apply to Scratch Orgs.

[23] 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.

[24] 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.

[25] The Salesforce Advanced Cross-Region Continuity (ACRC) offering enables recovery from events that disable all availability zones within a single region. ACRC's target recovery time objective and recovery point objective are 48 hours and 4 hours, respectively.

[26] 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.

Return of Customer Data[27]

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 of Customer Data for managed packages may not be available if the packages were removed prior to contract termination, as removing the package may begin the deletion process for associated Customer Data.

Deletion of Customer Data[28]

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. [29] 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

Important: Customers must use either Platform Encryption to encrypt the entire database (including standard and custom field values) via Tenant-Level Encryption and/or standard Platform Encryption to encrypt supported field types and file attachments, or the "classic encryption" custom fields feature, and manage the lifecycle of their encryption keys, when submitting payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords to the Covered Services. Customers may not otherwise submit such data to the Covered Services. For other categories of sensitive data, customers should also consider using Platform Encryption (including Tenant-Level Encryption, as necessary or desired) or "classic encryption."

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

---

[27] This section does not apply to Scratch Orgs. This section also does not apply to any Customer Data that has been encrypted using Platform Encryption Cache-Only Key Service or Encryption Key Management. Einstein Activity Capture and Salesforce Inbox do not support the export of Customer's activity data or insights generated on this activity data.

[28] This section does not apply to Scratch Orgs. As part of its system maintenance, SFDC will periodically delete any Scratch Org, including any associated data or Active Scratch Objects, as set forth in the Scratch Org Documentation. Deletion of an active Scratch Org shall not terminate Customer's Scratch Org subscription; if an active Scratch Org is deleted during Customer's Scratch Org subscription term, Customer may create a new active Scratch Org. Creation of new active Scratch Orgs count towards the daily scratch org limits set forth in the Scratch Org Documentation.

[29] 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.

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.

PGSSI-S. To the extent Customer is subject to Article L.1111-8 (or any successor thereto) of the French public health code (Code de la Santé Publique), Customer shall abide by the Global Information Security Policy for the Healthcare Sector (PGSSI-S) pursuant to Article L.1110-4-1 (or any successor thereto) of the aforementioned code.

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.

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 to create metrics showcasing the use of our services for marketing purposes. Any such metrics will be aggregated so as to not identify any individual or customer.

Processing of User Account Data

To create and administer user accounts and access the Covered Services, customers must provide information about users ("User Account Data"). User Account Data includes information such as name, username, business address, job title, country/region, phone number, and email. Salesforce processes User Account Data to provide its customers with the Covered Services; in that case, personal data about users is treated as Customer Data. Salesforce also processes User Account Data for certain of its own business purposes, such as account administration, invoicing, and licensing compliance, and treats it consistently with the Salesforce Privacy Statement.

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

SALESFORCE SERVICES
- For Sandboxes,[30] as part of its system maintenance, SFDC may delete any Sandbox that Customer has not logged into for 150 consecutive days. Thirty or more days before any such deletion, SFDC will notify Customer (via email, unless Customer opts out) that the Sandbox will be deleted if Customer does not log into it during that 30-day (or longer) period. Deletion of a Sandbox shall not terminate Customer's Sandbox subscription; if a Sandbox is deleted during Customer's Sandbox subscription term, Customer may create a new Sandbox.

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 FIELD SERVICE
- For Salesforce Field Service, any Customer Data submitted to AWS as part of the optional FS Optimizer or Enhanced Scheduling & Optimization functionality is retained in AWS for 30 days, after which it is securely overwritten or deleted.

SALESFORCE MAPS (INCLUDING MAPS LITE) AND SALESFORCE SALES PLANNING
- For Salesforce Maps and Salesforce Sales Planning, 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. Self-Hosted Data submitted to AWS are converted into data layer files, and the original CSV files are deleted after 90 days. Any Custom Data Sources returned pursuant to the "Return of Customer Data" section will be in the form of a converted data layer file, not the original CSV file.

MARKETING IN SALESFORCE STARTER
- Notwithstanding anything to the contrary contained herein, the Salesforce Security Guide is not applicable to Marketing in Salesforce Starter, ProSuite, or CRM Foundations.Notwithstanding anything to the contrary contained herein, the "Setup Audit Trail" (which allows customers to view

---

[30] Sandbox subscriptions are for testing and development use only, and not for production use.

and download certain administrative changes to the Covered Services) as described in the Security Policies and Procedures section above is not applicable to Marketing in Salesforce Starter, ProSuite, or CRM Foundations.

SALESFORCE MARKETING CLOUD SERVICES[31]
- Notwithstanding anything to the contrary contained herein, the [Salesforce Security Guide] is not applicable to the following Salesforce Marketing Cloud Services: Marketing Cloud Einstein, MC Advertising, and Marketing Cloud Engagement. For additional information on the security controls and user authentication for Salesforce Marketing Cloud Services, 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 Salesforce Marketing Cloud Services.
- After termination of the MC Advertising[32] 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 MC Advertising 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.
- Unified Messaging interoperates with products and features from Service Cloud, Sales Cloud, Experience Cloud, Enhanced Messaging, Marketing Cloud Growth Edition and/or Marketing Cloud Advanced Edition, and Data Cloud. The underlying Documentation for those products and features will apply, including the Einstein Platform Documentation where applicable.
- Marketing Cloud Growth Edition and Marketing Cloud Advanced Edition include products and features from the Salesforce Services, Data Cloud, Marketing Cloud Engagement, and Marketing Cloud Einstein and may interoperate with features from Enhanced Messaging. The underlying Documentation for these products and features will apply, including the Einstein Platform Documentation where applicable.
- Marketing Intelligence includes and interoperates with products and features from Data Cloud, Tableau Next, Marketing Cloud Einstein, and Agentforce. The underlying Documentation for such products and features will apply, including Einstein Platform Documentation..

TABLEAU CLOUD
- With respect to Disaster Recovery, the recovery time objective and recovery point objective times may be different than listed herein. Tableau Cloud Disaster Recovery information is described in the "Tableau Cloud Security, Privacy and Architecture" documentation available [here].
- With respect to Return and Deletion of Customer Data, information relating to Tableau Cloud is described in the"Tableau Cloud Security, Privacy and Architecture" documentation available [here].

---

[31] Salesforce Marketing Cloud Services refers to Covered Services that are listed as Marketing Cloud Services in the Trust and Compliance Documentation.
[32] In the case of MC Advertising services which are not terminated at the same time as Marketing Cloud Engagement services are terminated, customers may request deletion of Customer Data submitted to the MC Advertising services by contacting marketingcloudsupport@salesforce.com.

SERVICES ON THE HYPERFORCE OPERATING ZONE (FORMERLY EU OPERATING ZONE) INFRASTRUCTURE
- With respect to Covered Services on the Hyperforce Operating Zone infrastructure, in the following limited circumstances, Customer Data may be stored and/or processed outside of the European Union or Switzerland, as applicable:
  - To maintain the availability and performance of the Covered Services. In the event that regularly scheduled performance and availability testing of a Customer Org indicates a Customer Org is experiencing performance or availability issues, a limited set of Customer Data may be evaluated outside of the HF Operating Zone to resolve the error. Such Customer Data is limited to a copy of a Customer's Org configuration. No personal data is collected from standard Org configurations.
  - To detect, investigate, respond to, and remediate incidents impacting Customer Data, such as Customer Data Incidents as defined in Section 7 of the DPA.
  - If Customer provides Customer Data when engaging with Customer Support. Please note it is not necessary for Customer to provide Customer Data to log a support case or to obtain support.
  - HF Operating Zone support personnel may communicate via private Slack channels to resolve customer support cases that require collaboration between the HF Operating Zone support team. If Customer grants HF Operating Zone support personnel access to the Customer Org, Customer Data may be shared between HF Operating Zone support personnel in private Slack channel messages to resolve the Customer's support case. While processing of Slack messages may be done outside of the HF Operating Zone, Slack messages are encrypted at rest and in transit.
  - Some Content Delivery Networks ("CDNs")transfer and cache Customer Data at the CDN node hosted in various locations globally. Customers may request to enable connection to such CDNs by logging a support case or reaching out to the account team.
  - Salesforce may store and process Administrative Customer Data (as defined below) to assist in debugging, to provide Customer support, and to detect, investigate, and prevent security incidents. Administrative Customer Data is stored in the United States in environments that provide the appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss, alteration, damage, or access to, or unauthorized disclosure of, Administrative Customer Data), confidentiality, and integrity of Administrative Customer Data. "Administrative Customer Data" includes:
    - metadata supplied to Covered Services when connected with third party services a Customer may choose to use with the Covered Services as described above in the section titled "**Interoperation with Other Services**".
    - Setup metadata entered by Customer such as folder names, attachment names, names of custom objects, urls, and custom Apex code.
    - Search queries entered into the Covered Services (but not search results).
  - For the purposes of preventing fraud or abuse and to comply with applicable law, hosting provider AWS reserves the ability to access systems processing and storing encrypted Customer Data. Salesforce has implemented technical measures that prevent AWS from accessing unencrypted Customer Data and from accessing encryption keys used to encrypt Customer Data. With Platform Encryption, Customers may generate and store encryption key material outside of Salesforce.

- ○ In response to a legally binding request to disclose Customer Data for which Salesforce has exhausted all the available remedies as described in the Agreement.
- ○ When Customer provides private keys for serving custom domains with customer-provided HTTPS Certificates on Salesforce servers, those private keys may be stored in the United States. Prior to storage in the United States, private keys will be encrypted using key management systems located within the HF Operating Zone to prevent decryption outside the HF Operating Zone.

Salesforce Data 360 (AKA Customer Data Cloud) OR CUSTOMER DATA PLATFORM (FORMERLY BRANDED AS SALESFORCE CDP) (COLLECTIVELY FOR THIS SECTION "DATA CLOUD SERVICES")
- In the event Customer orders the Data Cloud Services for purposes of proof of concept testing and non-production use, and requests SFDC's assistance in the provisioning and demonstration of such Services ("Purpose"), then Customer shall: (1) ensure that any data submitted, or requested to be submitted, to the Services do not contain Personal Data (as defined in the Data Processing Addendum), and, to the extent any submitted data is derived from Personal Data, Customer must obfuscate such Personal Data, otherwise it may be rejected by SFDC and/or SFDC may refuse to provide such assistance; (2) when requesting SFDC personnel (including employees, contractors, and subcontractors of SFDC and its Affiliates) to access, use, demonstrate, or otherwise assist with Customer's use of the Covered Services for the Purpose, acknowledge that: (a) said SFDC personnel ("SFDC Users") shall be Users of Customer as defined in the MSA; and (b) said SFDC Users shall have access to any Customer Data being used within the Services for the Purpose based on the user permissions set by Customer; and (3) Customer shall not send SFDC or the SFDC Users any data via electronic mail.