Heroku Security, Privacy and Architecture

Published: September 11, 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.

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 branded as Heroku ("Heroku Services").

Architecture and Data Segregation

The Heroku 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 "Organization IDs" 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 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 Heroku Services.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to Heroku:

- **Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Heroku Services 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/.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Heroku Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce."
- **APEC Privacy Recognition for Processors (PRP):** Customer Data submitted to the Heroku 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/.

- **TRUSTe Certification**: Salesforce's Website Privacy Statement and privacy practices related to the Heroku 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.
- **ISO 27001/27017/27018 certification:** Salesforce operates an information security management system (ISMS) for the Heroku Services 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 the Heroku Services is available here.
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to Heroku Services undergoes an independent evaluation in the form of a SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available by logging a support ticket via https://help.heroku.com.
- **Payment Card Industry (PCI)**: For Heroku Shield Private Spaces, Shield Dynos, and Shield Heroku Postgres, Salesforce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council ("PCI DSS") as a data storage entity or third-party agent from an Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Heroku's AoC is available upon request from your organization's Salesforce account executive. Customers must use TLS 1.2 or greater when interacting with applicable services to benefit from Salesforce's PCI DSS AoC.
- **ASIP Santé certification:** Salesforce has obtained the French health data hosting certification (ASIP Santé certification) that enables Salesforce to host French health data for the Heroku Services. Salesforce's most recent ASIP Santé certification is available upon request from your organization's Salesforce account executive.

The Heroku 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 for the Heroku Services, the infrastructure used by Salesforce to host Customer Data submitted to the Heroku Services is provided by a third party, Amazon Web Services, Inc. ("AWS"). Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Security Controls

The Heroku Services include a variety of configurable security controls that allow customers to tailor the security of the Heroku Services for their own use. These controls include:

- Administrative access to applications built on the Heroku Services is controlled by configurable access lists. Customers can decide which accounts have access to application logs, configuration or data, or the ability to deploy new code.
- Each application built on the Heroku Services runs within its own isolated environment and cannot interact with other applications or areas of the Heroku Services. This restrictive operating

environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using Linux Containers (LXC) while host-based firewalls restrict applications from establishing local network connections.

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

Security Policies and Procedures

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

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID, resource accessed, 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 a customer or its ISP.
- If there is suspicion of inappropriate access, 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.
- Passwords are not logged.
- Salesforce personnel will not set a defined password for a user. If a user requests a password reset, Salesforce will deliver a temporarily valid, secret URL to the requesting user via email. A new password is set by visiting this URL.

Intrusion Detection

Salesforce, or an authorized independent third party, monitors the Heroku Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Heroku Services function properly.

Salesforce may conduct security scans and testing of customer code uploaded to the Heroku Services to detect abusive behavior or actions that violate terms for the Heroku Services.

Security Logs

All Salesforce systems used in the provision of the Heroku Services log information to their respective system log facilities or a centralized logging service (for network systems) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.

User Authentication

Access to the Heroku Services requires a valid user ID and password combination, which are encrypted via SSL/TLS while in motion and passwords are stored using a one-way salted hash. Alternatively, Heroku supports Single Sign On (SSO) utilizing SAML 2.0 which uses Public Key Encryption and does not require

Heroku to store a password. Following a successful authentication, a randomly-generated credential is transmitted to the user's browser or command line interface (CLI). All subsequent requests are authenticated with that credential.

Physical Security

Production data centers used to provide the Heroku Services have access system controls in place. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

Applications deployed on the Heroku Services and Customer Data submitted to the Heroku Services, up to the last committed transaction, are automatically replicated on a near real-time basis at the database layer and are backed up as part of the deployment process on secure, access controlled, and redundant storage.

Disaster Recovery

The Heroku Services utilize disaster recovery 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.

Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to a secondary data center utilizing developed operational and disaster recovery procedures and documentation.

For (1) Heroku Postgres and Heroku Redis plans that include the 'High Availability' option, (2) Heroku Private Spaces, and (3) Heroku Shield services*, there are disaster recovery plans with the following target recovery objectives: (a) restoration of the applicable Heroku Service within 12 hours after Salesforce's declaration of a disaster; and as applicable, (b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of multiple Availability Zones at the same time.

*Heroku Shield services include: Heroku Shield Private Spaces, Shield Dynos, Shield Heroku Postgres, Shield Connect, and Apache Kafka on Heroku Shield.

Viruses

Salesforce implements practices and software to limit the risk of exposure to software viruses.

Data Encryption

TLS is available as an option to be enabled for any web application running on the Heroku Services. Customer connections to Postgres databases via the Heroku Services require SSL encryption. Selected Heroku Postgres plans, as indicated in the Documentation, include encryption at rest.

Return of Customer Data

During the term of the agreement, customers may make copies of their respective Customer Data

submitted to the Heroku Services by following instructions here, here, or contacting support@heroku.com.

Deletion of Customer Data

Upon final termination of a customer database for any reason (such as account termination, customer deletion of the database, or other reason), Customer Data submitted to the Heroku Services is deleted within 30 days. This process is subject to applicable legal requirements.

Sensitive Data

Important: Customers must use Heroku Shield Private Spaces, Shield Dynos, and Shield Heroku Postgres when submitting payment cardholder data and authentication data, credit or debit card numbers, or any security codes to the Heroku Services in accordance with the PCI Data Security Standard and Heroku's PCI customer responsibility matrix. Customers may not otherwise submit such data to the Heroku Services.

Government issued identification numbers or bank account numbers may be submitted only to Heroku Private Spaces or Heroku Shield services (Heroku Shield services are identified in the "Disaster Recovery" section above). Customers may not otherwise submit such data to the Heroku Services.

Additionally, for the Heroku 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 Heroku Services, then Customer is responsible for ensuring that its use of the Heroku Services to process that information complies with all applicable laws and regulations.

For clarity, the foregoing restrictions do not apply to financial information provided to Salesforce for the purposes of checking the financial qualifications of, and collecting payments from, customers, the processing of which is governed by Salesforce's Website Privacy Statement.

Analytics

Salesforce may track and analyze the usage of the Heroku Services for purposes of security and helping Salesforce improve both the Heroku Services and the user experience in using the Heroku 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.

Interoperation with Other Services

The Heroku 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 Heroku 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.