HEROKU SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: May 6, 2016

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 data submitted by customers to our services ("Customer Data").

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").

Third-Party Architecture

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"). Currently, with the exception of Heroku private spaces offerings, the infrastructure hosted by AWS in the provisioning of the Heroku Services is located only in the United States and Ireland.

Audits and Certifications

EU/US and Swiss/US Safe Harbor self-certifications: Customer Data submitted to the Heroku Services is within the scope of an annual self-certification to the EU/US and Swiss/US Safe Harbor frameworks as administered by the U.S. Department of Commerce. The current self-certification is available at https://safeharbor.export.gov/list.aspx by searching for "Heroku."

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.

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 Procedures, Policies and Logging

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 LXC while host-based firewalls restrict applications from establishing local network connections.

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the Heroku Services for unauthorized intrusions. 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.

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 promptly notifies impacted customers of any actual or reasonably suspected 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 transmission. 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 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. Further information about physical security provided by AWS is available from the AWS Security Web site, including AWS's overview of security processes.

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 remote from their primary data centers, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centers were to be rendered unavailable.

Viruses

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

Data Encryption

Transport layer security (TLS) is available as an option to be enabled for any web application run on the Heroku Services. Customer connections to postgres databases via the Heroku Services require SSL encryption.

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 or contacting support@heroku.com. Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Heroku Services by contacting support@heroku.com.

Deletion of Customer Data

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

Sensitive Personal Data

Important: The following types of sensitive personal data may not be submitted to the Heroku Services: government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); information related to an individual's physical or mental health; and information related to the provision or payment of health care.

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 the Heroku Privacy Statement.

Tracking and Analytics

Salesforce may track and analyze use 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. Without limiting the foregoing, Salesforce may

share data about Salesforce's customers' or their users' use of the Heroku Services ("Usage Statistics") to Salesforce's service providers for the purpose of helping Salesforce in such tracking or analysis, including improving its users' experience with the Heroku Services, or as required by law.

Interoperation with Other Salesforce Services

The Heroku Services may interoperate with other services provided by Salesforce. The Security, Privacy and Architecture documentation for such services is available in the Trust and Compliance Documentation section of help.salesforce.com.