Audience Studio Security, Privacy and Architecture

Published: May 7, 2021

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's Master Subscription Agreement.

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the Services branded as Audience Studio and Data Studio (formerly branded as Salesforce DMP and Salesforce Data Studio and prior to that as Krux), or Services sold under a Krux Order Form (collectively, the "Audience Studio Services").

Architecture and Data Segregation

The Audience Studio Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors are subject to regular audits. The "Infrastructure and Sub-processors" documentation describes the sub-processors and certain other entities material to Salesforce's provision of the Audience Studio Services.

Third-Party Functionality

The Audience Studio Services may use third-party providers, other than AWS, to provide analytics or security, which providers may store logs describing usage of the Audience Studio Services. Additionally, a portion of customer support for the Audience Studio Services is provided using third-party technology, which may contemplate data, including screenshots of customers' instances of the Audience Studio Services, being hosted on the third-party's architecture.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Audience Studio Services:

- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Audience Studio 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. The current certification is available at https://www.privacyshield.gov by searching under "Salesforce."
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to the Audience Studio Services undergoes an independent evaluation in the form of a SOC 2 Type II report. Salesforce's most recent SOC 2 report for Audience Studio is available upon request from your organization's Salesforce account executive.
- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for Audience Studio in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's Salesforce account executive.
- **EU and UK Binding Corporate Rules (BCR) for Processors**: Customer Data submitted to the Audience Studio Services is within the scope of the Salesforce EU and UK BCR for Processors. The most current versions of the Salesforce EU and UK BCR for Processors are available on Salesforce's website, currently located at https://www.salesforce.com/company/privacy/.
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the Audience Studio Services is within the scope of Salesforce's PRP certification under the APEC Privacy Framework. The current certification is published in the PRP Compliance Directory at http://cbprs.org/compliance-directory/prp/.

Additionally, the Audience Studio Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and/or application security assessments, on at least an annual basis.

As further described in the "Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by a third party, Amazon Web Services, Inc. ("AWS"), to host Customer Data submitted to the Audience Studio Services. 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 Website.

Security Controls

The Audience Studio Services include a variety of security controls. These controls include:

- Unique user identifiers (user IDs) to help ensure that activities can be attributed to the responsible individual;
- Password length controls, with expiration;
- Password complexity requirements for Web and mobile access to the Audience Studio Services;
- Two-Factor Authentication for access by the Audience Studio Services to its third-party hosting services;
- Multi-Factor Authentication and Single Sign-On for access to the Audience Studio Services as set forth in the applicable Notices and License Information (NLI); and
- Web and mobile access to the Audience Studio Services via authorization and authentication frameworks.

Security Policies and Procedures

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

- User passwords are stored using a salted hash format and are not transmitted unencrypted;
- User access log entries will be maintained, containing date, time, URL executed or entity ID operated on, operation performed (viewed, edited, etc.), 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;
- Logs are stored securely to prevent tampering;
- Passwords are not logged;
- No defined passwords are set by Salesforce;
- Authentication tokens are encrypted and not transmitted unencrypted; and
- Access to Audience Studio Services servers is only granted via access keys (such as SSH or AWS IAM).

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

Intrusion Detection

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

Security Logs

All Salesforce systems used in the provision of the Audience Studio Services log information to a centralized syslog server (for network systems) or AWS's CloudTrail system (for agentless AWS services) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains 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 Audience Studio Services, directly or via the Audience Studio API, requires a valid user ID and password combination, or an API key/secret, both of which are encrypted via TLS while in transmission. Every user ID is associated with exactly one customer. For API access, each request requires authentication and authorization and is tied to a specific customer and user session. Once authenticated, all requests are required to have a valid session ID unique to the customer ID.

Physical Security

Salesforce is responsible for physical security measures at the Corporate Offices. Public cloud service providers are responsible for the security of the production data centers.

Reliability and Backup

All networking components, load balancers, web servers, and application servers are architected for global resilience. Customer Data submitted to the Audience Studio Web UI is stored on geographically disparate cloud data systems for higher availability. All Customer Data submitted to the Audience Studio Web UI is backed up daily. All Customer Data submitted to the Audience Studio Services is stored on highly durability and redundant network storage service supplied by AWS.

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 the Audience Studio Services back online within a brief period of time.

Viruses

The Audience Studio Services have controls in place that are designed to prevent the introduction of viruses to the Audience Studio Services.

Data Encryption

The Audience Studio Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data, which is encrypted in transit when uploaded to or downloaded from Audience Studio-created applications using Transport Layer Security 1.2 (TLS). TLS is active on all accounts by default.

Return of Customer Data

Within 30 days post contract termination, customers may request an export copy of Customer Data by contacting help@krux.com. The data available for export is subject to the customer's lookback window in the associated Order Form.

Deletion of Customer Data

After termination of the Audience Studio Services, following the 30-day period for return of Customer Data, Customer Data submitted to the Audience Studio Services is securely overwritten or deleted within 90 days. This process is subject to applicable legal and regulatory requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Audience Studio Services, Audience Studio reserves the right to reduce the number of days it retains such data after contract termination. Audience Studio will update its Security, Privacy and Architecture Documentation in the event of such a change.

Personal Data and Sensitive Data

Important: Customers may not submit personal data to the Audience Studio Services, except that customers may submit pseudonymous personal data and IP addresses. In addition, as the Audience Studio adheres to the Network Advertising Initiative (NAI) Code of Conduct, the Audience Studio Services may not be used (i) to associate pseudonymous device-identified information with other personal data in violation of the NAI Code of Conduct (https://www.networkadvertising.org/code-enforcement/code) and/or (ii) to use cookies, web beacons, or other tracking mechanisms to collect or store personal data in violation of the NAI Code of Conduct. For clarity, the NAI Code of Conduct applies to activities that occur in the United States or that apply to United States users.

Sensitive data that is regulated by data protection laws or regulations may not be submitted to the Audience Studio Services, including but not limited to, government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); information, including inferences, pertaining to an individual's health or medical condition; information pertaining to sexual orientation, or religion; and data defined as Sensitive Information under either the NAI Code of Conduct or the Self-Regulatory Principles for Online Behavioral Advertising of the Digital Advertising Alliance. For clarity, aforementioned sensitive data may also not be submitted in a pseudonymized way. Furthermore, the Audience Studio Services may not be used to select or target advertising based on past visits or clicks by users or on sites directed at children (in accordance with applicable law or regulations governing targeted advertising of children. e.g. the NAI Code of Conduct terms are applicable to under thirteen (13) years of age).

For clarity, the foregoing restrictions do not apply to information provided to Salesforce for the purposes of 1) establishing user accounts for use of the Audience Studio Services or 2) checking the financial qualifications of, and collecting payments from, Salesforce's customers, the processing of which is governed by the Web Site Privacy Statement for the Audience Studio Services.

Analytics

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

Salesforce uses Customer Data in an aggregated and anonymized form to create a data set (the "Anonymized Data"). No Customer Data consisting of personal data is contained in the Anonymized Data, nor any data that would identify customers, their users, customers' consumers, or any individual, company or organization. Salesforce may combine the Anonymized Data with that of other customers to create marketing reports and to provide product features. By using the Audience Studio Services, customers consent to the creation of reports based on the Anonymized Data.

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 Audience Studio 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 Audience Studio 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.