Professional Services Security, Privacy and Architecture

Published: December 17, 2024

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 Professional Services Customer Information, which for purposes of this document means electronic data constituting Confidential Information, including Personal Data, provided by or for Customer to Salesforce under a Professional Services Agreement ("Agreement"). All capitalized terms not defined herein shall have the meaning set forth in the Agreement and the Professional Services Data Processing Addendum ("PSDPA").

Services Covered

This documentation describes the architecture of, and the administrative, technical and physical controls applicable to Professional Services performed under the Agreement or under an SOW or an Order Form that incorporates this Professional Services Security, Privacy and Architecture Documentation or a PSDPA.

Architecture and Data Segregation

The Professional Services are operated in a manner designed to segregate and restrict Professional Services Customer Information access based on business needs. Our processes provide logical data separation for different customers and, depending on the Professional Services, may allow the use of customer and user role-based access privileges.

Control of Processing

Salesforce has implemented procedures designed to ensure that Personal Data is processed as instructed by the customer, throughout the 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.

Salesforce Enterprise-Level Corporate Environment

Controls applicable to certain aspects of the Professional Services (e.g. asset management, employee training, and hiring practices) are covered by Salesforce's common enterprise-level controls applicable to Salesforce's company-wide corporate environment ("Salesforce's Corporate Environment"). The following security and privacy-related audits and certifications are applicable to Salesforce's Corporate Environment, as described below:

- **ISO 27001/27017/27018 certification**: Salesforce operates a formal, documented information security management system (ISMS) for common enterprise-level controls applicable to Salesforce's company-wide corporate environment (referred to as "SF Corporate" in the Statement of Applicability) in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018 (with the exclusion of certain Online Services). 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.

- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment for common enterprise-level controls applicable to Salesforce's company-wide corporate environment (referred to as Salesforce's "Corporate Services" in the SOC reports) undergo an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402) or SOC 2. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available for download on Salesforce's compliance website.

Security Controls

All Salesforce workstations (which, as used herein, refer to laptop and desktop computers provided by Salesforce to its personnel) that are used to perform Professional Services (each, a "Workstation") are protected by measures designed to ensure the confidentiality and integrity of Professional Services Customer Information, including the following:

- Application and operating system patches and services packs are kept up-to-date, either automatically or via a centrally controlled process.
- A real-time virus scanner is installed and running; signature files are kept up-to-date; the virus scanner runs a daily scan of the Workstation.
- An anti-spyware solution is active; signature files are kept up-to-date; anti-spyware scans are run at least weekly.
- Full disk encryption using the Advanced Encryption Standard (AES) with a minimum key length of 128 bits.
- Access to a Workstation requires the user to enter their unique user ID and password. All Salesforce users are required to keep and maintain complex passwords. Salesforce corporate network passwords are set to a minimum of 12-character alphanumeric passwords.
- User access to the Salesforce corporate network requires multi-factor authentication.
- Salesforce has and shall maintain policies that prohibit the use of personally-owned workstations for the processing of Professional Services Customer Information by Salesforce employees.
- Workstations are documented and tracked in a formal asset management system.

Security Policies and Procedures

Professional Services are provided in accordance with the following policies and procedures to enhance security:

- Salesforce users are required to change their passwords at regular intervals, and may not use the three most recently used passwords. Passwords are treated as Confidential Information.
- Salesforce users are required to maintain uniquely identifiable user IDs to ensure accountability for all activities, actions, and access to Professional Services Customer Information.
- Salesforce limits its use of Professional Services Customer Information it receives when providing Professional Services to that appropriate to providing its services to Customer.
- Salesforce personnel who have access to Professional Services Customer Information are informed of the confidential nature of the Professional Services Customer Information through appropriate training on their responsibilities with respect to access to such types of information.
- All Salesforce employees providing Professional Services must complete annual mandatory security and privacy training. Completion is tracked by Salesforce.

Network Configuration

Salesforce's internal network, which may be used to process Professional Services Customer Information, is protected by the following safeguards:

- Firewalls to control access between the Internet and Workstations used to process Professional Services Customer Information.
- Salesforce corporate wireless networks are configured to utilize WPA2, at a minimum, for wireless security, and Salesforce shall maintain a materially equivalent or stronger configuration for wireless security during the performance of Professional Services.
- Application and operating system patches and services packs are kept up-to-date on network equipment, either automatically or via a centrally controlled process in accordance with a formal patching policy, and are hardened according to defined configuration standards that restrict unnecessary services and ports.

Incident Management

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

Security Logs

Salesforce has and shall maintain system event logging procedures for Workstations and Salesforce internal network systems that access or store Professional Services Customer Information, namely: (a) event logs for all security devices, perimeter devices, and policy enforcement points (including firewalls, VPN servers, and intrusion detection systems); (b) network log-on records from authentications systems, including domain controller logs.

Return and Deletion of Personal Data

Salesforce has implemented policies and procedures designed to ensure that Personal Data will not be stored on Workstations or other physical media provided by Salesforce and used to perform Professional Services, unless necessary to provide Professional Services.

Excluding any Personal Data that may have been, at Customer's instruction, submitted to the Online Services and that is now Customer Data as defined in Customer's MSA, upon request by Customer after the effective date of termination or expiration of the relevant SOW or Order Form (the "Expiration Date"), Salesforce will make the Personal Data in its possession or control available to Customer, to the extent applicable, for return, export or download for a period of 30 days after the Expiration Date. Salesforce will otherwise have no obligation to maintain any Personal Data.

Upon Customer's instruction, Salesforce will delete Personal Data in its possession or control, unless legally prohibited.

Sensitive Data

Important: Customer is responsible for ensuring that its provision of sensitive or regulated data to Salesforce, if any, along with its related processing instructions, are compliant with all applicable laws and regulations. Salesforce makes no representation that its Professional Services are compliant with laws related to sensitive or specially regulated data, including without limitation government-issued identification numbers; financial information (such as credit or debit card numbers, bank account numbers, and any related security codes or passwords); personal health information; or other data subject to special legal requirements.

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 Privacy Statement.

Third-Party Tools

Salesforce's Sub-processors include third-party cloud tools that may be used in the performance of the Professional Services and which Process Personal Data, e.g. those listed in Salesforce's Infrastructure and Sub-processors Documentation for Professional Services.Salesforce may also use other third-party tools that do not qualify as Sub-processors, including tools that Process Personal Data at Customer's instruction, that are entirely on-premise, or that do not Process Personal Data.