((sirenum))

Security and Privacy

Information Sheet

((sirenum))

Sirenum dynamic workforce management technology is among the most secure in the industry. With experience in high-compliance industries like temporary staffing and transportation, Sirenum's founders had security and compliance high on their list of qualities the software should possess. For that reason, Sirenum was built on Salesforce, whose robust security and privacy programs meet the highest standards in the industry. Sirenum is a Salesforce ISV partner, which subjects us to regular security reviews ensuring our product is compliant with Salesforce's high standards.

Architecture

The Salesforce Services are operated in multi-tenant architecture that is designed to segregate and restrict access to customer data based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. 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.

Security Controls

The Salesforce Services include a variety of security controls, policies and procedures, as further described in our Trust and Compliance Documentation. Salesforce, or an authorized independent third party, monitors the Salesforce Services for unauthorized intrusions using network-based intrusion detection mechanisms. The Salesforce Services use, or enable customers to use, industry-accepted encryption products to protect customer data and communications during transmissions between a customer's network and the Salesforce Services, including through Transport Layer Encryption (TLS) leveraging 2048-bit RSA server certificates. Production data centers used to provide the Salesforce Services have access control systems that permit only authorized personnel to have access to secure areas.

Certifications

Salesforce operates an information security management system ("ISMS") for the Salesforce Services in accordance with the ISO 27001 international standard and aligned to ISO 27018. Salesforce has achieved ISO 27001/27018 certification for its ISMS from an independent third party. Salesforce's information security control environment applicable to the Salesforce Services has undergone an independent evaluation in the form of SOC 1, SOC 2 and SOC 3 audits. Salesforce also has been awarded the TRUSTe Certified seal signifying that Salesforce's Website Privacy Statement and privacy practices related to the Salesforce Services are compliant with TRUSTe's Certification Standards. Additionally, the Salesforce Services regularly undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

((sirenum))

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Salesforce services on which Sirenum is built.

- **Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the services branded as Sales Cloud, Service Cloud, Chatter, Community Cloud and Force.com is within the scope of the Salesforce BCR for Processors (except when hosted on the Public Cloud Infrastructure). The most current version of the Salesforce BCR for Processors is available on Salesforce's website, currently located at http://www.trust.salesforce.com.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification:** Customer Data submitted to the Covered 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."
- **ISO 27001/27017/27018 certification:** Salesforce operates an information security management system (ISMS) for the Covered 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 Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's Salesforce account executive.
- **Service Organization Control (SOC) reports:** Salesforce's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of 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 upon request from your organization's Salesforce account executive.
- **TRUSTe certification:** Salesforce has been awarded the TRUSTe Certified seal signifying that Salesforce's Website Privacy Statement and privacy practices related to the Covered Services have been reviewed by TRUSTe for compliance with TRUSTe's Certification Standards.
- **Payment Card Industry (PCI):** For the Covered Services, 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 a Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of Salesforce's AoC is available upon request from your organization's Salesforce account executive. 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.
- **HITRUST certification:** For the Covered Services (excluding IoT Explorer (including IoT Plus), Salesforce CPQ and Billing, and Einstein Discovery), Salesforce has obtained HITRUST CSF Certification. A copy of Salesforce's HITRUST letter of certification is available upon request from your organization's Salesforce Account Executive.
- **ASIP Santé certification:** 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 Covered Services with the exclusion of Messaging. Additionally, the Covered Services undergo security assessments by internal personnel and third parties on at least an annual basis.

Source: trust.salesforce.com