Security, Privacy and Architecture of the Vlocity-Managed Packages
Published: August 31, 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 following Vlocity-branded managed package offerings: (i) Vlocity Communications package, (ii) Vlocity Media and Entertainment package, (iii) Vlocity Energy & Utilities or Vlocity Commodity package, (iv) Vlocity Insurance package, (v) Vlocity Health package, and (vi) Vlocity Government package (collectively, the “Covered Services”). For clarity, this documentation does not apply to other Vlocity offerings, including without limitation, Order Management Plus or Digital Commerce Gateway.

The Covered Services are provisioned as managed packages on Customer’s existing Salesforce service; the Customer installs and runs the Covered Services on the underlying Salesforce service. The Security, Privacy, and Architecture Documentation applicable to the Salesforce Services describes the controls applicable to Customer Data processed in connection with the Covered Services, except as set forth in this documentation.

If the underlying Salesforce service is Government Cloud Plus, the Government Cloud Plus Security, Privacy, and Architectures Documentation does not apply to the Covered Services, and instead the Salesforce Services Security, Privacy, and Architecture Documentation will apply.

Architecture and Data Segregation
The Covered 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 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 Covered Services.
Third-Party Functionality
Certain features of the Covered Services use functionality provided by third parties. The National Plan and Planning Enumeration System (NPPES) feature in the Covered Services uses third-party services to access and capture content relating to National Provider Identifier information. Customers must enable this feature to use this functionality.

Audits and Certifications
The Audits and Certifications set forth in the Security, Privacy, and Architecture Documentation applicable to the Salesforce Services do not apply to the Covered Services; instead the following security- and privacy-related audits and certifications are applicable to the Covered Services, as described below:

- **Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Covered 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/](https://www.salesforce.com/company/privacy/).
- **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 Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in the Vlocity Privacy Shield Notice. The current certification is available at [https://www.privacyshield.gov/list](https://www.privacyshield.gov/list) by searching under “Vlocity.”

Additionally, the current generally available version of the Covered Services undergoes security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Disaster Recovery, Return of Customer Data, and Deletion of Customer Data
Disaster Recovery, Return of Customer Data, and Deletion of Customer Data for Customer Data processed in connection with the Covered Services are described in the Disaster Recovery, Return of Customer Data, and Deletion of Customer Data sections of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services, except as follows:

The Disaster Recovery, Return of Customer Data, and Deletion of Customer Data sections of the Security, Privacy, and Architecture Documentation applicable to the Salesforce Services may not be applicable to the Covered Services if the Covered Services were removed before contract termination because Customer Data may have been deleted at the time the managed package was removed.

Additional Security, Privacy, and Architecture Information
Additional Security, Privacy, and Architecture information applicable to Customer Data processed in connection with the Covered Services are described in the following sections of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services:

- Security Controls
- Security Policies and Procedures
- Intrusion Detection
- Security Logs
- Incident Management
- User Authentication
- Physical Security
- Reliability and Backup
- Viruses
- Data Encryption
- Sensitive Data
- Analytics, and
- Interoperation with Other Services