Vlocity 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 (A) 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 "Managed Package Services"), (B) the Vlocity-branded offerings referred to as Digital Commerce Gateway (the "Digital Commerce Services"), and (C) the Vlocity-branded offerings referred to as Order Management Plus (the "Order Management Plus Services", and collectively with the Managed Package Services and the Digital Commerce Services, the "Covered Services").

The Managed Package Services are provisioned as managed packages on Customer's existing Salesforce service; the Customer installs and runs the Managed Package 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 Managed Package 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 Managed Package Services, and instead the Salesforce Services Security, Privacy, and Architecture Documentation will apply.

Architecture and Data Segregation

The Managed Package 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. The Digital Commerce Services and Order Management Plus Services are operated in an architecture providing logical data separation for different customers via customer-specific accounts. For the Covered Services, 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 Managed Package Services use functionality provided by third parties. The National Plan and Planning Enumeration System (NPPES) feature in the Managed Package 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:

- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Managed Package Services and Order Management Plus 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/.
- **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 by searching under "Vlocity."
- **System and Organization Controls (SOC) reports:** Salesforce's information security control environment applicable to the Digital Commerce Services and Order Management Plus Services undergoes an independent evaluation in the form of a SOC 2 audit. The most recent SOC 2 report is available upon request.

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.

As further described in the "Infrastructure and Sub-processors" documentation, Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process Customer Data submitted to the Digital Commerce Services and the Order Management Plus Services. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the AWS Security website and the AWS Compliance website.

Security Controls

Security Controls for Customer Data processed in connection with the Managed Package Services are described in the Security Controls section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Security Controls for Customer Data processed in connection with the Digital Commerce Services and the Order Management Plus Services, the Digital Commerce Services and the Order Management Plus

Services use AWS, as described above; further information about security provided by AWS is available from the AWS Security website, including AWS's overview of security processes.

Security Policies and Procedures

Security Policies and Procedures for Customer Data processed in connection with the Managed Package Services are described in the Security Policies and Procedures section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

The Digital Commerce Services and Order Management Plus Services are operated in accordance with the following policies and procedures to enhance security:

- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) 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 Customer or its ISP.
- If there is suspicion of inappropriate access, Salesforce can provide customers log entry records for use in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs and system infrastructure logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Certain administrative changes to the Digital Commerce Services are tracked and are available for viewing or download by a customer's system administrator upon request.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Managed Package Services function properly.

Security Logs

Security Logs for Customer Data processed in connection with the Managed Package Services are described in the Security Logs section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Security Logs for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, all systems used in the provision of the Digital Commerce Services and Order Management Plus Services log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Incident Management for Customer Data processed in connection with the Managed Package Services are described in the Incident Management section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Incident Management for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, Salesforce maintains security 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. Salesforce typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Salesforce's response.

User Authentication

User Authentication for Customer Data processed in connection with the Managed Package Services are described in the User Authentication section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For User Authentication for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, access to Digital Commerce Services and Order Management Plus Services requires authentication via one of the supported mechanisms as described in the Salesforce Security Guide, including user ID/password, SAML-based Federation, or OAuth as determined and controlled by the Customer.

Physical Security

Physical Security for Customer Data processed in connection with the Managed Package Services is described in the Physical Security section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Physical Security for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, production data centers used to provide the Digital Commerce Services and Order Management Plus Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

Reliability and Backup for Customer Data processed in connection with the Managed Package Services are described in the Reliability and Backup section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Reliability and Backup for Customer Data processed in connection with the Digital Commerce Services, all networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Digital Commerce Services is stored on a primary database server with multiple failover servers for redundancy. The foregoing replication and backups may not be available to the extent the Customer has spun down the applicable Digital Commerce Services cache cluster.

For Reliability and Backup for Customer Data processed in connection with the Order Management Plus Services, all networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Order Management Plus Services is stored on a primary database server with multiple failover servers for redundancy. All Customer Data submitted to the Order Management Plus Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Order Management Plus Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to regionalized data stores. Backups are verified for integrity and stored in the same region as their instance.

Disaster Recovery

Disaster Recovery for Customer Data processed in connection with the Managed Package Services are described in the Disaster Recovery section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services, except as follows:

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

For Disaster Recovery for Customer Data processed in connection with the Digital Commerce Services, 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. The Digital Commerce Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable. In the event of a disaster impacting Customer Data in the Digital Commerce Services, the Customer Data will remain available within the Salesforce Services and a new cache can be rebuilt using this Customer Data. The foregoing does not apply to development and testing environments.

For Disaster Recovery for Customer Data processed in connection with the Order Management Plus Services, 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. The Order Management Plus Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable. Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation. The Order Management Plus Services' disaster recovery plans currently have a target recovery objective of 4 hours for maximum Customer Data loss (recovery point objective).

Viruses

Virus scanning for Customer Data processed in connection with the Managed Package Services are described in the Viruses section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Virus scanning for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, the Digital Commerce Services and Order Management Plus Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Digital Commerce Services or Order Management Plus Services by a customer.

Data Encryption

Data Encryption for Customer Data processed in connection with the Managed Package Services is described in the Data Encryption section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Data Encryption for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, the Digital Commerce Services and Order Management Plus Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Digital Commerce Services and the Order Management Plus Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across encrypted links utilizing AES-256 encryption.

Return of Customer Data

Return of Customer Data for Customer Data processed in connection with the Managed Package Services is described in the Return of Customer Data section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services, except as follows:

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

For Return of Customer Data for Customer Data processed in connection with the Digital Commerce Services, the Digital Commerce Services cache Customer Data submitted by Customer to the Managed Package Services. Customers may request return of the Customer Data submitted to the Digital Commerce Services through the same Return of Customer Data process applicable to the Managed Package Services (to the extent such data has not been deleted by Customer, or if Customer has not already removed the managed package in which the Customer Data was stored). Salesforce shall provide such Customer Data via downloadable files in comma separated value (.csv) format and attachments in their native format. If the Managed Packages Services were removed before contract termination, the Customer Data may have been deleted at the time the managed package was removed.

For Return of Customer Data for Customer Data processed in connection with the Order Management Plus Services, Customers may request return of the Customer Data submitted to the Order Management Plus Services through the same Return of Customer Data process applicable to the Managed Package Services (to the extent such data has not been deleted by Customer, or if Customer has not already removed the managed package in which the Customer Data was stored). If the Managed Packages Services were removed before contract termination, the Customer Data may have been deleted at the time the managed package was removed.

Deletion of Customer Data

Deletion of Customer Data for Customer Data processed in connection with the Managed Package Services is described in the Deletion of Customer Data section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services, except as follows:

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

For Deletion of Customer Data for Customer Data processed in connection with the Digital Commerce Services, Customer Data used in connection with the Digital Commerce Services is retained for 30 days, except to the extent that Customer modifies such retention period. Once the default or Customer-set retention period has expired, the AWS cache processing Customer Data will shut down, overwriting or deleting such Customer Data. Without limiting the ability for customers to request return of their Customer Data submitted to the Digital Commerce Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Salesforce Security, Privacy and Architecture Documentation in the event of such a change.

For Deletion of Customer Data for Customer Data processed in connection with the Order Management Plus Services, Customer Data used in connection with the Order Management Plus Services is securely overwritten or deleted from production within 60 days, and from backups within 180 days. This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Order Management Plus Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Salesforce Security, Privacy and Architecture Documentation in the event of such a change.

Sensitive Data

Sensitive Data for Customer Data processed in connection with the Managed Package Services are described in the Sensitive Data section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Sensitive Data for Customer Data processed in connection with the Digital Commerce Services, Customers may not submit payment cardholder data and authentication data, credit or debit card numbers, any security codes or passwords, personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, or any other sensitive or regulated data to the Digital Commerce Services. If Customer does submit personal health information or other sensitive or regulated data to the Digital Commerce Services, then Customer is responsible for ensuring that its use of the Digital Commerce Services to process that information complies with all applicable laws and regulations. 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 Website Privacy Statement.

For Sensitive Data for Customer Data processed in connection with the Order Management Plus Services, Customers must use the attribute encryption functionality provided by the Order Management Plus Services when submitting payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords to the Order Management Plus Services. Customers may not otherwise submit such data to the Order Management Plus Services. For other categories of sensitive data, customers should also consider using “Platform Encryption” or “Classic Encryption.”

Additionally, for the Order Management Plus Services, the following types of sensitive personal data may not be submitted: personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, except in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission contractually. Notwithstanding the foregoing, any Customer using Public Cloud Infrastructure may not submit to the Order Management Plus Services Protected Health Information, as defined under the U.S. Health Insurance Portability and Accountability Act. If Customer does submit personal health information or other sensitive or regulated data to the Order Management Plus Services, then Customer is responsible for ensuring that its use of the Order Management Plus Services to process that information complies with all applicable laws and regulations. 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 Website Privacy Statement.

Analytics

Analytics for Customer Data processed in connection with the Managed Package Services are described in the Analytics section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Analytics for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, Salesforce may track and analyze the usage of the Digital Commerce Services Order Management Plus Services for purposes of security and of helping Salesforce improve both the Digital Commerce Services and the user experience in using the Digital Commerce Services and Order Management Plus Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Interoperation with Other Services

Interoperation with Other Services for Customer Data processed in connection with the Managed Package Services is described in the Interoperation with Other Services section of the Security, Privacy and Architecture Documentation applicable to the Salesforce Services.

For Interoperation with Other Services for Customer Data processed in connection with the Digital Commerce Services and Order Management Plus Services, the Digital Commerce Services and Order Management Plus Services may interoperate or integrate with other services provided by Salesforce or third parties. When third-party systems connect to the Digital Commerce Services and Order Management Plus Services, these external systems supply metadata to the Digital Commerce Services and Order Management Plus Services for the purpose of maintaining the intended functionality of the integration, for example an external system may supply a third-party record ID, file name, folder name, or similar label intended to identify a record that is being sent to the Digital Commerce Services. Salesforce may collect and store such metadata to ensure product functionality, and to assist in debugging, support and for security purposes. Salesforce provides appropriate protections for such metadata and treats it consistently with our Privacy Statement.

Salesforce 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 Digital Commerce Services and Order Management Plus 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.