B2C Commerce/Commerce Cloud 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 B2C Commerce or Salesforce Commerce Cloud (formerly "Demandware"), which includes Commerce Cloud Digital (B2C Commerce GMV or B2C Commerce PPO) , Commerce Cloud Einstein (including services formerly branded by Demandware, Inc. as Predictive Email), and B2C Commerce Order Management[1] (collectively, the "B2C Commerce Services"), provided by salesforce.com, inc. or Demandware, LLC, a salesforce.com, inc. company ("Salesforce"), but excluding those services branded as Retail.net and/or Tomax. Some of the elements described in this documentation, such as audits and certifications, reliability and backup, intrusion detection, and disaster recovery, do not apply to sandboxes or any other developer or testing environments. For clarity, however, the Sensitive Data section below, including the restrictions on submission of sensitive data, apply to all environments.

Architecture and Data Segregation

The B2C Commerce 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 those 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 B2C Commerce Services.

[1] Any reference to "B2C Commerce Order Management" in this documentation refers to the version of Order Management released prior to February 19, 2020. For versions of Order Management released on or after February 19, 2020 ("Salesforce Order Management"), please see the Salesforce Services documentation here.

Third-Party Functionality

Salesforce may use third parties to protect the B2C Commerce Services from Distributed Denial of Services ("DDoS") attacks. If an attack occurs, a third party may be used to identify and block malicious online traffic. Information about website traffic and the targeted website may be accessed by the third party to enable these functions.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to one or more of the B2C Commerce Services, as described below:

- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the B2C Commerce Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks 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."
- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the B2C Commerce 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/.
- **Payment Card Industry (PCI)**: For the Commerce Cloud Digital and B2C Commerce Order Management Services, Salesforce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry 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 through the Salesforce Compliance Portal. Customers must use Commerce Cloud platform provided encryption methodologies for supported field types when storing personal account numbers ("PAN" or "credit card numbers") to benefit from Salesforce's PCI DSS AoC.
- **ISO 27001/27017/27018**: Salesforce operates an information security management system (ISMS) for the B2C Commerce Services in accordance with the ISO 27001 international standard and aligned to ISO 27017 and 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The scope of Salesforce's ISO 27001/27017/27018 certification applicable to Commerce Cloud Digital, Commerce Cloud Einstein and B2C Commerce Order Management services and certificate are available upon request from your organization's Salesforce Account Executive.
- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to the Commerce Cloud Digital services undergoes an independent evaluation in the form of a SOC 1 (SSAE 18 / ISAE 3402) audit. Additionally, Salesforce's information security control environment applicable to Commerce Cloud Digital, Commerce Cloud Einstein and B2C Commerce Order Management capabilities, undergoes an independent evaluation in the form of SOC 2 and SOC 3 audits. These reports are available upon request from the Salesforce Compliance Portal.
- **TRUSTe certification**: Salesforce's Website Privacy Statement and privacy practices related to the B2C Commerce Services are assessed by TRUSTe annually, for compliance with TRUSTe's Certification and Verification Assessment Criteria. For more information on the status of Salesforce's certification/verification status, click here.
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the B2C Commerce 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/.

The B2C Commerce Services undergo 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, some infrastructure used by Salesforce to host Customer Data submitted to the B2C Commerce Services is provided by a third party, Amazon Web Services, Inc. ("AWS"). Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Web site and the AWS Compliance Web site.

Security Controls

B2C Commerce Services include a variety of configurable security controls for the customer's authorized administrators on the B2C Commerce Services platform. These controls include but are not limited to the following:

- Various user access management controls.
- Various password complexity controls.
- User access logs for the Customer's instance are available for review and export, where applicable.
- Multi-factor Authentication for customer code uploads.
- Multi-factor Authentication and Single Sign-On for access to the B2C Commerce Services as set forth in the applicable Notices and License Information (NLI).
- IP-level restriction for application level access

Security Policies and Procedures

The B2C Commerce Services are operated in accordance with the following policies and procedures to enhance security:

- User passwords are not transmitted unencrypted.
- User passwords are stored encrypted or as a derived secret key.
- Log files for the Customer's instance are available for review and export, where applicable.
- Internal system accounts are reviewed on a regular basis.
- Logs are stored securely.
- Passwords are not logged unless specifically configured by the Customer.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the B2C Commerce 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 for incident detection and response, to prevent fraudulent authentication of customer accounts, and to ensure that the B2C Commerce Services function properly.

Security Logs

All Salesforce systems used in the provision of the B2C Commerce Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized log collection server in order to enable security reviews and analysis.

Incident Management

Salesforce maintains a security incident management program. 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

The B2C Commerce Services allow Customers to customize many logical access management controls to provision and manage access. Access to Commerce Cloud Services requires a valid user ID and password combination, which are encrypted via TLS while in transmission. Passwords are passed through key-derivation function and the secret keys are stored by the B2C Commerce Services. For B2C Commerce Order Management, passwords are encrypted.

Physical Security

Production data centers used to provide the B2C Commerce Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by guards, multi-layered access controls, video surveillance, and are also supported by on-site backup generators in the event of a power failure.

For B2C Commerce Services using AWS, further information about physical security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Reliability and Backup

The B2C Commerce architecture is designed to be highly redundant and reliable. Should a customer's primary data center encounter a disaster that prevents it from functioning, formal processes are in place to restore the customer's production-level B2C Commerce Services. Customer Data submitted to the B2C Commerce Services is stored on a primary database server with a replicated copy for high availability and performance. All Customer Data submitted to the B2C Commerce Services, up to the last committed transaction, is automatically replicated daily to another location.

Disaster Recovery

Salesforce has disaster recovery plans in place for the B2C Commerce Services and tests those plans at least annually. In the event that production facilities for the B2C Commerce Services hosting the customer's primary data center were to be rendered unavailable, redundant hardware, software, and equipment are in place.

Viruses

The B2C Commerce Services have controls in place that are designed to prevent the introduction of viruses to the B2C Commerce Services.

Data Encryption

The B2C Commerce Services enable customers to use industry accepted encryption products to protect Customer Data and communications during transmissions to the B2C Commerce Services.

Salesforce offers PCI-DSS compliant encryption for supported payment field types at rest and in transit. Functionality is made available to Customers to encrypt additional data, if required.

Return of Customer Data

The B2C Commerce Services allow import, export or deletion of Customer Data by authorized users. In some cases, Customers may purchase subscriptions to more than one environment which have different Order End Dates. Following termination or expiration of a subscription, the customer has 30 days to access its account and download or export Customer Data from the applicable environment that is subject to the termination or expiration. For questions regarding the return of your Customer Data, contact the Commerce Cloud support organization.

Deletion of Customer Data

Following the 30-day period for Customers to download or export their Customer Data, Salesforce will promptly deprovision the customer environment. Salesforce shall then have no obligation to maintain or provide any Customer Data, and all Customer Data in its systems or otherwise in its possession or under its control shall be subject to deletion. Notwithstanding the foregoing, certain data relating to the usage and performance of Customer's website will be retained for analytics purposes after termination ("Analytics Data"). The Analytics Data will not include any personal data.

Sensitive Data

Important: The following types of sensitive personal data may not be submitted to the B2C Commerce Services: Government-issued identification numbers.

When submitting payment card data or other sensitive user authentication data to the B2C Commerce Services, Customers are responsible for ensuring that sensitive data, such as payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords submitted to the B2C Commerce Services is encrypted, whether it is through the Commerce Cloud platform provided encryption methodologies, the customer's encryption methodologies, or a third-party's encryption methodologies. Customers may not otherwise submit such data to the B2C Commerce Services.

Additionally, for the B2C Commerce 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.

If Customer does submit personal health information or other sensitive or regulated data to the B2C Commerce Services, then Customer is responsible for ensuring that its use of the B2C Commerce Services to process that information complies with all applicable laws and regulations.

The types of sensitive personal data as described above may not be submitted to sandboxes or any other developer or testing environments. Please contact your customer support manager for further information regarding submission of sensitive personal data to the B2C Commerce Services.

Analytics

Salesforce may track and analyze the usage of the B2C Commerce Services for purposes of security and of helping Salesforce improve both the B2C Commerce Services and the user experience. 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.

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.

In addition, Salesforce may, for purposes reasonably required to develop, deliver, and provide ongoing innovation to the B2C Commerce Services and other Salesforce Services use Customer Data on an aggregate or anonymous basis ("Anonymized Data") and use Customer Data relating to Customer's website (s) ("Website Data"), including data derived from website management, use of the website, and catalogue data. The Anonymized Data may also be used for marketing and benchmarking, as well as for other research and analysis. None of the resulting Anonymized Data, nor any such Website Data will include personally identifiable information. For clarity, in no event does Salesforce share Customer Data with any other customers. By using the B2C Commerce Services, customers consent to this use of their Customer Data.

Interoperation with Other Services

The B2C Commerce Services may interoperate or integrate with other services provided by Salesforce. The Security, Privacy, and Architecture documentation for such services 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 B2C Commerce 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.