UPDATED NOVEMBER 2019

This document provides information about the privacy and security of the B2C Commerce (formerly Commerce Cloud) Services which can help our customers to assess our security and privacy program, including by completing privacy impact assessments. It does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation. More information about privacy impact assessments can be found here.

GDPR and B2C Commerce

At Salesforce, trust is our #1 value, and nothing is more important than the success of our customers and the protection of their data. Salesforce enables our customers to build trusted relationships, putting their customers at the center of everything they do, including protecting individual privacy through GDPR compliance.

The General Data Protection Regulation (GDPR) is a comprehensive European privacy law effective May 25, 2018. The GDPR expanded the privacy rights of EU individuals and places new obligations on all organizations that market, track, or handle EU personal data. For more information about the GDPR, please refer to our Salesforce GDPR website, specifically our GDPR Key Facts paper, which defines a number of the terms used in this document.

Salesforce is committed to complying with the GDPR in providing services to our customers as a processor and to both ensuring that our customers can continue to use our services while complying with the GDPR. Similar to existing privacy laws, compliance with GDPR requires a partnership between Salesforce and our customers in their use of our services. As part of our commitment to our customers, we've published this document to describe the features customers can use when responding to common GDPR requests using the B2C Commerce Services, and to assist our customers in completing their data protection impact assessment for B2C Commerce Services. Capitalized terms not defined herein have the meaning set forth in Salesforce's Master Subscription Agreement and/or Data Processing Addendum.

[1] This document covers the services branded as Commerce Cloud Digital (B2C Commerce GMV or B2C Commerce PPO), Commerce Cloud Einstein (including services formerly branded Predictive Email), and Order Management, together the "B2C Commerce Services." This document does not apply to other services such as Retail.net or Tomax.

Security

GDPR requires organizations to use appropriate technical and organizational security measures to protect Personal Data against unauthorized processing and accidental disclosure, access, loss, destruction, or alteration. The B2C Commerce Services have robust security and privacy programs in place that meet the highest standards in the industry. They help Salesforce's customers to comply with a variety of data protection laws and regulations applicable to Salesforce's services. The B2C Commerce Services are operated in a multi-tenant 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. 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.

The B2C Commerce 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 B2C Commerce Services for unauthorized intrusions using network-based intrusion detection mechanisms. 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. Production data centers used to provide the B2C Commerce Services have access control systems that permit only authorized personnel to have access to secure areas.

Salesforce operates an information security management system (ISMS) for the B2C Commerce Services in accordance with the ISO 27001 international standard. Salesforce has achieved ISO 27001 certification for its ISMS from an independent third party. The scope of Salesforce's ISO 27001 certification applicable to the Commerce Cloud Digital and Order Management Services is available here. Salesforce's information security control environment applicable to Commerce Cloud Digital, as well as Einstein and Order Management, capabilities undergoes an independent evaluation in the form of SOC 2 and SOC 3 audits. Salesforce also has been awarded the TRUSTe Certified seal signifying that Salesforce's Commerce Cloud Website Privacy Statement and privacy practices related to the B2C Commerce Services have been reviewed by TRUSTe for compliance with TRUSTe's Certification Standards. Additionally, 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.

Data Subject Rights

The GDPR grants European Union (EU) individuals, or data subjects under the GDPR, a number of rights in respect of how organizations handle their personal data. These rights require organizations to have systems in place to respond to and effectively address data subjects' requests. For example, if an individual submits a request to have its personal data deleted and the relevant circumstances apply, companies must be equipped to find the relevant personal data linked to that individual and delete it. Salesforce B2C Commerce Services enable customers to process these requests by using functionality within the products. The B2C Commerce Services enable customers to develop and manage e-commerce websites. As such, when describing the functionality available in the B2C Commerce Services, we will refer to individuals or data subjects as "shoppers."

Basis of Data Processing and Right to Object: In order to process personal data, companies must have a lawful basis to process the data. Under the GDPR, there are six legal bases which organizations can rely on to lawfully process personal data. One basis for processing is with the consent of the data subject (the five other bases are (i) legitimate interest, (ii) contractual necessity, (iii) compliance with legal obligations, (iv) vital interest and (v) public interest). It is up to each Salesforce customer to determine which legal basis is most appropriate for their processing operations, and if they choose to rely on consent, obtain the appropriate consents from their data subjects. Consent under the GDPR must be freely given, specific, fully informed and an unambiguous indication of the data subject's wishes by clear affirmative action. Data subjects can, in certain cases, object at any time to the processing of their personal data, in particular if the processing is for direct marketing purposes.

- It is up to each Salesforce customer to determine the basis on which it processes Personal Data, and if required, to obtain appropriate consent from the shopper. Customers are in the best position to determine the proper scope of consent required due to the customizations made and the third parties that each customer may have integrated with.

- Salesforce has a new "Do Not Track" flag for the Digital Script API for Session to give merchants the tools to manage their own storefront consent management solution.

Data Access and Data Portability: Data subjects have the right to confirm with a data controller whether the organization is processing their personal data. If it is, the data controller must provide the data subject with information about such processing, including the specific data processed, the purposes of the processing, and the other parties with whom such personal data has been shared. In certain cases, data subjects have the right to ask a controller to provide their personal data in a structured, commonly used, and machine-readable format so that they can transmit their own personal data to another company.

- Shoppers can request to obtain certain personal data in a structured, machine-readable format so they can transmit relevant data to another company. Salesforce provides merchants the ability to offer a self-service data export to shoppers using a new data export cartridge.
- Commerce Digital customers are able to export Personal Data and then delete it via Business Manager.
  - Einstein Customers are able to export Personal Data via API and then delete the Personal Data by submitting requests in Business Manager.
  - Order Management Customers are able to export Personal Data via API and then anonymize the Personal Data via API or within the Order Management user-interface.
- Most account data is already directly available to customers to copy into a portable file. Commerce Cloud Digital and Order Management provide a number of APIs and user-interfaces that allow customers of the Commerce Cloud Service to access and export shopper Personal Data. Customers can then provide that information to their shoppers or other third parties.

Data Rectification: Data Subjects can request that a controller correct or complete personal data if the data is inaccurate or incomplete.

Each Commerce Cloud Service allows customers to modify data about their shoppers, such as changing contact information, in response to a shopper's request.

Right to Erasure: Also known as "the right to be forgotten," this right empowers data subjects to request that a controller delete or remove their personal data in situations such as the following: when the data is no longer needed for the original purpose, when the data subject withdraws consent, or when the data subject objects to the processing and the data controller has no overriding legitimate interest in the processing.

- A shopper can ask the Commerce Cloud customer (the data controller) to delete Personal Data, using lines of communication established by the customer to receive such requests. Customer can honor those requests for the B2C Commerce Services as follows:
  - For Commerce Cloud Digital, customers have the ability to delete their own shopper Customer Data in the services.

  - For Commerce Cloud Einstein, all Customer Data is automatically deleted from the Commerce Cloud Einstein Services regularly, and will not be retained longer than 13 months.

  - The deletion capabilities and documentation available in the Infocenter cover all Personal Data subject to the Right of Erasure. Customers can submit deletion requests in Business Manager and/or via API with respect to shopper data, custom objects, tracking data, and analytics data. Order Management customers will be able to delete the Personal Data in the OMS product itself and/or via API.

- If a Salesforce customer needs assistance to delete Personal Data that it has submitted to the B2C Commerce Services, Salesforce will provide assistance as described in its contract with the customer. Salesforce's current Data Processing Addendum is available here.

Restriction of Processing: Data Subjects can request that a controller stop access to and modification of their personal data. For example, the controller can mark or use technological means to ensure that such data will not be further processed by any party.

- To restrict processing of a shopper's Personal Data in the B2C Commerce Services, a customer may export the Personal Data and then delete it from the B2C Commerce Services. The customer may retain the exported Personal Data without processing it further until the restriction is lifted. Once the restriction is lifted, the shopper can re-establish a new profile.

Answers to Common Data Protection Impact Assessment Questions about the B2C Commerce Services

I. SCOPE

This document is designed to help customers by providing information they can use to complete their own privacy impact assessments or data protection impact assessments about their use of the B2C Commerce Services.

II. OVERVIEW OF PERSONAL INFORMATION

Provide a general description of the Service.

The B2C Commerce Services are a software-as-a-service solution. It is a hosted service that enables companies to develop and manage customizable, easy-to-use e-commerce websites. The B2C Commerce Services include Digital, the main hosted website service; Order Management, an add-on feature that allows companies to manage their transaction records; and Commerce Cloud Einstein, which allows companies to use artificial intelligence technology to enhance their e-commerce operations.

Describe the personal data that will be used, stored, collected, disclosed or otherwise Processed on the Service.

B2C Commerce customers choose what data to submit to, and collect with, the B2C Commerce Service. Typical personal data processed would include information about the customer's personnel who use the service (login credentials, contact information, activity records, etc.) and information about the shoppers who visit the customer's B2C Commerce-hosted website and create accounts or perform transactions (contact information, activity records, transaction records, etc.).

Does the Personal Data include "special categories of Personal Data" (as defined under GDPR) or Personal Data related to criminal convictions or offences?

B2C Commerce customers could submit most "special categories of Personal Data" to the

Service, but submission of these types of data are not required or part of the expected use case. Customers are contractually prohibited from submitting health-related information (which is a "special category") to the B2C Commerce (unless Salesforce has expressly permitted submission of health-related information) as described in the Security, Privacy, and Architecture Documentation, available here.

Does the Personal Data include financial account numbers, government identification numbers, or health information?

Customers can choose whether to submit financial information consisting of payment card data or other sensitive user authentication data to the B2C Commerce Service; if they do so, they are responsible for ensuring such Personal Data is encrypted, and they can encrypt the Personal Data using B2C-provided tools. Customers are contractually prohibited from submitting government-issued identification numbers to the B2C Commerce, (and should submit health-related information only with Salesforce's express permission) as described in the Security, Privacy, and Architecture Documentation available here.

Where are the Data Subjects located?

This depends on how the B2C Commerce customer uses the B2C Commerce Service. For example, the locations of Data Subjects will depend on: (1) what information the B2C Commerce customer submits to the Service; (2) where the B2C Commerce customer's Users of the B2C Commerce Service are located; and (3) the countries from which the B2C Commerce customer's shoppers access the customer's B2C Commerce-hosted website.

What is the general purpose for Processing the Personal Data?

The Salesforce B2C Commerce Service is a hosted service that enables companies to develop and manage customizable, easy-to-use e-commerce websites. Thus, the B2C Commerce Service is typically used by customers to provide an e-commerce platform to online website visitors and to process e-commerce transactions. The B2C Commerce customer, as the data controller, should determine its specific purpose for processing Personal Data on the Service. Salesforce processes Personal Data to offer the B2C Commerce Service, under the terms agreed in its contract with the B2C Commerce customer.

Could the Processing of the Personal Data have an impact on key aspects of an individual’s life?

How Salesforce’s Processing of Personal Data affects key aspects of an individual’s life will depend upon the B2C Commerce customer’s use case.

Are the Data Subjects made aware of the details of the Processing of their Personal Data?

Salesforce provides self-service tools that its customers are able to use to interact with their Data Subjects. Thus, Salesforce does not directly communicate with its customers’ Data Subjects, and ensuring Data Subjects’ awareness is the B2C Commerce customer’s responsibility. To the extent Data Subjects are interested in Salesforce’s specific practices, Salesforce’s Privacy Statement and other privacy-related documentation are available here.

III. ACCESS TO Personal Data

How is Personal Data managed in the Service?

The B2C Commerce Service’s user interface allows customers to manage their own B2C Commerce-hosted websites, and B2C Commerce customers manage the Personal Data in the B2C Commerce Service. To the extent customers need Salesforce’s assistance in managing Personal Data, Salesforce has committed to provide assistance as described in its Data Processing Addendum. The current version of Salesforce’s Data Processing Addendum is available here.

How is access to the B2C Commerce Service managed?

B2C Commerce customers can assign access to their Users. The B2C Commerce Service also allows role-based permissions, so customers can assign access permissions based on the User’s role. Salesforce’s customer contracts restrict access by Salesforce’s personnel, who may access Personal Data only to provide the B2C Commerce Service, to prevent or address technical or service problems, as compelled by law, or as the customer expressly permits in writing.

Can Salesforce personnel access Personal Data on the B2C Commerce Service? If so, where are those personnel located and for what purpose do they need access?

Salesforce agrees by contract that its personnel may access Personal Data only in accordance with Customer’s documented instructions for specific purposes, including processing under the contract, processing initiated by the customer in using the services, and processing to comply with *other instructions provided by the customer. The locations of Salesforce's Affiliates that employ personnel who may access Personal Data for these purposes is available in the Infrastructure & Sub-processors Documentation, available here.*

Who will manage security of the B2C Commerce Services?

Salesforce has policies and procedures in place to protect the security of the B2C Commerce Services. The security policies, procedures and controls that Salesforce makes available to B2C Commerce customers are described in the B2C Commerce Security, Privacy and Architecture Documentation, available here. B2C Commerce customer share responsibility for managing security. The B2C Commerce Service includes a variety of security controls that the B2C Commerce customer can configure; each customer is responsible for configuring those security controls and for managing other aspects of processing under its control such as the security of the customer's end users' computers, and controlling access to its instance of the Service.

Who is responsible for assuring proper use of the Personal Data?

Customers are responsible for using the Services appropriately, including their processing of Customer Data on the B2C Commerce Services. Salesforce is responsible for providing the B2C Commerce Services appropriately under its contract with its customers. Under that contract, Salesforce commits to using the Personal Data only in accordance with Customer's documented instructions for specific purposes, including processing under the contract, processing initiated by the customer in using the services, and processing to comply with other instructions provided by the customer.

How can requests from individual Data Subjects to access or correct their Personal Data be handled on the B2C Commerce Services?

The Service allows customers to manage the Personal Data they maintain in the B2C Commerce platform, including in response to Data Subject requests. To the extent a customer needs Salesforce's assistance to respond to a Data Subject, Salesforce will provide assistance as described in its Data Processing Addendum, available here.

IV. INFORMATION SYSTEM DESIGN

Where will Personal Data be stored?

Salesforce's storage locations for Personal Data are described in the Infrastructure and Sub-processors Documentation, available here.

Will the Personal Data be stored in the European Union?

Under the GDPR, there is no requirement for personal data to be stored in the European Union (EU). As outlined in the preceding question, the B2C Commerce Services storage locations are described in the Infrastructure and Sub-processors Documentation, available here, and in some cases a Customer may have data servers located in the EU. In addition, Salesforce offers two mechanisms to legally transfer personal data outside of the EU for the B2C Commerce Services: the EU-US and Swiss-US Privacy Shield certification, and the Standard Contractual Clauses. For more information about these transfer mechanisms and which B2C Commerce Services will rely on which mechanism, please review the Salesforce's Data Processing Addendum.

Describe the B2C Commerce Services' information flow for personal data.

The B2C Commerce Service is a cloud-based platform, and customers can allow their Users to access the B2C Commerce Service from virtually anywhere with an internet connection. Customers may also receive website visitors from around the world. For these reasons, personal data may flow to or from B2C Commerce to global locations, depending on where the customer, its Users, or its website visitors are located.

In terms of data flows within the Service:

- Personal data about a B2C Commerce customer's users: Customers enter personal data about their users when they provision the users' accounts. Personal data may also be collected when users perform activities on the services–for example, when their actions generate records of their activities. In either case, the information flows from the location of the person entering the data to the B2C Commerce's storage facilities. If Customers wish to access or delete data about their users and their use of the B2C Commerce Services, they should contact Support for assistance.

- Personal Data about a B2C Commerce customer's website visitors: Information about website visitors is collected as the visitor performs activities on a B2C Commerce customer's website. In this case, the information flows from the visitor's location to the B2C Commerce's storage facilities.

- <u>Personal Data accessed by Salesforce personnel:</u> If Salesforce personnel access Personal Data– for example, if a customer requests that Salesforce access its data during a customer support inquiry– the data will be visible to the Salesforce individual accessing the data. The locations of Salesforce and its sub-processors are described in the Infrastructure and Sub-processors documentation available here.

How are transfers across national borders accounted for? If a transfer takes place, what is the purpose of this transfer?

Salesforce's Data Processing Addendum, available here, offers multiple transfer mechanisms for the B2C Commerce Services and includes an "order of precedence" clause. Specifically, Salesforce offers both EU-US and Swiss-US Privacy Shield certification, and the Standard Contractual Clauses for the B2C Commerce Services.

How (and with whom) will Personal Data be shared on the Services?

Personal Data is shared with Salesforce and, if applicable, its sub-processors, as described in the Infrastructure and Sub-processors Documentation, available here. Access by Salesforce and its sub-processors is subject to the protections in the Data Processing Addendum available here, and Salesforce maintains safeguards to prevent access except (a) to provide the Service and prevent or address service or technical problems, (b) as compelled by law, and (c) as the B2C Commerce customer expressly permits in writing.

What contracts are in place to protect Personal Data submitted to the B2C Commerce Service?

Protections for Personal Data are described in the B2C Commerce customer's contract with Salesforce. Contractual documents containing protections for Personal Data include (1) a Master Subscription Agreement (MSA) between Salesforce and the customer; (2) Salesforce's Data Processing Addendum (DPA), which can be added to the contract (if not already included) by following the instructions here; (3) and the Trust and Compliance Documentation, available here.

V. SECURITY AND DATA INTEGRITY

What technical security and physical security measures are in place to protect Personal Data from unauthorized access or disclosure?

Salesforce's policies and procedures to protect the security of Personal Data, and configurable security controls available to the B2C Commerce customer, are described in the B2C Commerce Security, Privacy and Architecture Documentation available here.

How are breach notifications addressed?

Salesforce has comprehensive procedures in place to notify customers in the event of a data breach of its systems as managed by its Computer Security Incident Response Team (CSIRT). Salesforce commits contractually in its GDPR-ready Data Processing Addendum to notifying customers "without undue delay" which is the standard of notification required for processors under the GDPR. Salesforce has a formal Incident Management Process that guides the Salesforce Computer Security Incident Response Team (CSIRT) in investigation, management, communication, and resolution activities.

Salesforce will promptly notify the Customer in the event of any security breach of the Salesforce Services resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce Support, email to the customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system.

Can Personal Data be masked or anonymized?

Yes. As described in the B2C Commerce Security, Privacy, and Architecture Documentation, available here, the B2C Commerce Service encrypts data in transit and allows customers to encrypt some data at rest. Order Management Customers can anonymize order information in the product itself or via API.

VI. RETENTION/DISPOSAL OF INFORMATION

How long is Personal Data retained on the B2C Commerce Service?

Customers choose how long to retain Personal Data on the B2C Commerce Service. Unless otherwise specified in the Documentation, Salesforce does not delete Customer Data, including Personal Data, during a subscription term, unless the customer instructs Salesforce to do so. After a customer's contract with Salesforce terminates, Salesforce deletes Personal Data in the manner described in the Security, Privacy and Architecture Documentation, available here.

How is Personal Data disposed of when it is no longer needed?

Upon request by the customer, or after termination of a customer's contract, Salesforce deletes the customer's Personal Data from the B2C Commerce Service in the manner described in the Security, Privacy and Architecture Documentation, available here. For the Commerce Cloud Einstein services, which apply predictive intelligence to help customers manage their e-commerce websites, data is deleted automatically within 13 months.

How are requests from Data Subjects to have their Personal Data deleted managed?

As described in Salesforce's Data Processing Addendum, available here, Salesforce shall notify its customer if it receives a request to exercise rights related to the processing of Personal Data on the B2C Commerce Services (for which that customer is the Data Controller). The B2C Commerce Services provide functionality to enable the customer to respond to that request, but Salesforce's Data Processing Addendum also commits to provide reasonable assistance if needed.

VII. MISCELLANEOUS

Has Salesforce appointed a Data Protection Officer?

Yes. Lindsey Finch is Salesforce's Data Protection Officer. She can be reached at privacy@salesforce.com.

Does Salesforce have a Privacy Policy?

Yes, Salesforce's privacy statements are available here.

Please provide an overview of how Salesforce incorporates the principles of "privacy by design" into its product development.

Salesforce works to incorporate privacy and data protection concepts from the inception of each new service or feature it offers. Product managers and engineers who design our products are trained at least annually on data protection. In addition, each Salesforce service is supported by at least one product attorney knowledgeable about data protection generally, and the GDPR in particular, and who reviews and advises on the product's functionality. Additionally, each product attorney is supported by a privacy attorney who specializes in data protection. The product release cycle also contains multiple checks where additional people can provide comments on the service or feature's protection of Personal Data. Finally, when a service or feature is released, it is described in the product documentation and release notes so that customers can perform their own evaluations. Salesforce regularly considers input from its customers when designing and refining product functionality.

Please provide details of how Salesforce is addressing its accountability and governance obligations under the GDPR.

Salesforce commits to meeting its accountability and governance obligations under the GDPR and will take all appropriate related measures. These measures include implementing appropriate technical and organizational security measures (more details available in the Trust and Compliance documentation), undertaking privacy impact assessments (where appropriate) and maintaining records of processing, among others. Salesforce will also appoint a data protection officer as is required under the GDPR.

Are Salesforce employees bound by confidentiality obligations?

Yes, Salesforce commits in its GDPR-ready Data Processing Addendum to ensure that personnel have been appropriately trained, are reliable and enter into confidentiality agreements. Employees also regularly undergo data protection training, such as the European Union Privacy Law Basics Trailhead.