UPDATED NOVEMBER 2019

This document provides information about the privacy and security of the Salesforce 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 the Salesforce Services

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 European privacy law that went into effect on 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 both complying with the GDPR in providing services to our customers as a processor and to 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 Salesforce Services, and to assist our customers in completing their data protection impact assessment for the Salesforce 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 Sales Cloud, Service Cloud, Community Cloud, Chatter,Lightning Platform (including Force.com), Site.com, and the Salesforce Platform underlying all of the above (known as the "Salesforce Platform") (collectively, the "Salesforce Services"). This document also covers the packages branded as Employee Apps, App Cloud or Lightning Platform. This document does not apply to other Salesforce services that may be associated with or integrate with the Salesforce Services, such as Einstein Discovery, Einstein Vision, Quip, Salesforce Inbox, IoT Cloud, Marketing Cloud, DMP, and Salesforce LiveMessage.*

Security

The 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. Salesforce has robust security and privacy programs in place that meet the highest standards in the industry. They enable us to comply with a variety of data protection laws and regulations applicable to Salesforce.

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 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 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 (SSAE 18 / ISAE 3402), 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, Salesforce has obtained an Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry (PCI) Data Security Standard (DSS), the HITRUST CSF Certification, the ASIP Santé certification - the French health data hosting certification that enables Salesforce to host French health data, the German Cloud Computing Compliance Controls Catalogue (C5) certification and the Japan CS Gold certification for the Salesforce Services.

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.

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 subject 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. The Salesforce Services enable customers to process these requests by using the following tools within the products.

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.

- The Salesforce Platform provides tools to customers to assist them in implementing custom objects to capture an individual's consent, where required. For more information about custom objects, please see this Trailhead module providing an overview of how "objects" and "fields" are used within Salesforce.

- Customers may also store individual preferences in data privacy records using the Individual object, which was made available in the Spring 18 release. These preferences include, for example, "do not track", "do not process" and "forget me", among others, and this functionality can be tied to contacts, person accounts, leads, and users. Note, however, that although the data privacy records let you track and store certain data privacy preferences and tie them to contacts, person accounts, leads, and users, it's up to customers to determine how to honor those preferences.

COMMON EXAMPLES INCLUDE THE FOLLOWING:

- Customers may wish to seek consent from their Users for email-read receipts as part of the Sales Cloud product offering. Since customers currently use read-receipts in different ways, customers will be able to instruct administrators to enable or disable read receipts at the organizational level.
- If an individual no longer wishes to receive sales-related calls or emails, for example, their contact details can be deleted in those lead records and the "email opt-out" and "do not call" options can be selected.
- In addition, if a customer checks the "email opt-out" flag on a lead or contact record, then the contact or lead will be excluded from all mass emails. If a User wishes to compose an individual email to that contact or lead, they will see that the contact or lead has opted out in the user interface, which indicates additional discretion is needed.
- The same concept applies to the use of Lightning Dialer; if customers check the the "do not call" flag on a contact or lead record, and a User attempts to call that individual, they will receive an error message.
- For Field Service Lightning Mobile, technicians can use the operating system settings on their mobile phones to opt out of location-based tracking. Administrators can turn off location tracking for mobile app users and exclude certain individuals from geo-location tracking.

For more details about consent management and the Salesforce Services, please see the Help Documentation.

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 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 subject 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.*

- For the Salesforce Services editions Enterprise, Performance, Unlimited, Developer, and Database.com, the Salesforce Services will allow customers to provide portable copies of Personal Data to individuals who request it. Salesforce offers the ability to export Personal Data via several methods, including through the application programming interface ("API") and the Salesforce Service's user interface. The process involves identifying and exporting Personal Data in a structured format (and if required later, deleting that Personal Data).
- For the Salesforce Services edition Salesforce Essentials and most Professional editions, Personal Data may be exported via reports, and/or the data management option under Setup.

For more details about data portability in the Salesforce Services, please see the Help Documentation.

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

- Each Salesforce Services product allows customers to modify data about individuals, such as changing contact information, in response to an individual's request.

Right to Erasure: *Also known as "the right to be forgotten," this right empowers data subjects to request that a data 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 controller has no overriding legitimate interest in the processing. A data subject can request personal data be deleted from the data controller through the lines of communication that the data controller sets up to accept such requests.*

- In the Salesforce Services, customers have the capability to delete both structured Customer Data (meaning highly organized data, such as data associated with an individual's user name) and unstructured Customer Data (meaning data that does not have a pre-defined model, such as Personal Data contained in a Chatter post). Contacts, leads and most other records can be deleted through the Salesforce user interface or an API.

- The ability to remove the personal information of an individual and replace the content fields with meaningless values, such as "redacted user," is also available for circumstances in which the Personal Data cannot be deleted (for example, a Chatter profile). For this type of Personal Data, the Personal Data can be masked by changing the data on the user record itself. For example, the email address could be changed to deleteduser@delete.myco.com.

- After a customer's contract with Salesforce terminates, Salesforce deletes all Customer Data, including Personal Data, in the manner described in the Salesforce Services Security, Privacy and Architecture documentation, available here.

For more details about the right to erasure in the Salesforce Services, please see the Help Documentation.

Restriction of Processing: *Data subjects can request that a data controller block or suppress the processing of their personal data. For example, the data controller can mark or use technological means to ensure that such data will not be further processed by any party. This may be relevant if a customer wants to temporarily restricts processing operations until their records are updated or in the case of a legal hold being placed on certain records.*

- A customer administrator can use APIs to export the relevant Personal Data out of their instance of the Salesforce Services and hold that data in a file outside of it. Next, the administrator should delete the relevant Personal Data from the instance. Once the restriction(s) have been lifted the customer administrator can re-import the relevant Personal Data into the instance.

For more details about the right to restriction in the Salesforce Services, please see the Help Documentation.

Answers to Common Data Protection Impact Assessment Questions about the Salesforce 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 Salesforce Services.

II. OVERVIEW OF PERSONAL INFORMATION

Provide a general description of the Service.

Salesforce provides its customers with software-as-a-service solutions, including the following services covered in this document:

- **Sales Cloud**, a customer relationship management (CRM) platform designed for managing accounts, contacts, opportunities, leads, and sales records;
- **Service Cloud**, a customer service platform that allows users to create, manage, and resolve cases, and to customize and automate workflow and approvals;
- **Community Cloud**, a platform for building and hosting communities for customers, partners, and employees, where individuals can ask questions, find answers, and share information;
- **Chatter**, an enterprise social network that allows a Salesforce customers' users to interact and support one another within Salesforce; and
- **Salesforce Platform**, a development platform that allows customers to build and run their own intelligent apps in Salesforce (and Site.com and Database.com, which are predecessors).

These services are built on Salesforce's proprietary Salesforce Platform, and benefit from the security and data protection features that the Salesforce Platform offers.

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

Salesforce customers choose what data to submit to, and collect with, the Salesforce Services.

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

Salesforce customers may be able to submit most "special categories of Personal Data" to the Salesforce Services, but submission of those types of data is not required nor part of the expected use case. Further details about the types of special categories of Personal Data that Salesforce customers are permitted to submit to the Salesforce Services is in the Security, Privacy, and Architecture Documentation available here. Salesforce customers are responsible for ensuring that submission of special categories of Personal Data complies with applicable laws.

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

Customers can choose whether to submit financial information to the Salesforce Services; if they do so, they are responsible for ensuring this submission complies with any applicable laws, such as in certain cases, encryption. Customers should submit payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords to the Salesforce Services only as described in the Security, Privacy, and Architecture Documentation available here. Salesforce customers may also submit health-related information to the Salesforce Services except where prohibited by the Security, Privacy and Architecture Documentation, and may submit government identification numbers. Salesforce customers are responsible for ensuring that the submission of special categories of personal data complies with laws.

Where are the Data Subjects located?

The answer depends on how the Salesforce customer uses the Salesforce Services. For example, the locations of Data Subjects will depend on: (1) what information the Salesforce customer submits to the Service; (2) where the Salesforce customer's authorized users of the Salesforce Services are located; and (3) the countries from which the Salesforce customers' consumers access any Salesforce-hosted application or website.

What is the general purpose for Processing the Personal Data?

Salesforce provides online software-as-a-service tools for sales, customer service, and community-building, as well as analytics tools and a cloud Salesforce Platform for application development. Thus, the Salesforce Services are typically used by Salesforce's customers to interact with their own customers and manage the information surrounding those interactions. The Salesforce customer, as the data controller, should determine its specific purpose for processing Personal Data on the Salesforce Services. Salesforce processes Personal Data to offer the Service, under the terms agreed in its contract with the Salesforce 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 Salesforce 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 customers are able to use to interact with their Data Subjects. Thus, Salesforce does not directly communicate with its customers' Data Subjects, and Data Subjects' awareness of the data processing is the Salesforce 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?

Salesforce's user interface allows customers to manage their own Customer Data, including Personal Data, on the Salesforce Services. 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 Service managed?

Salesforce customers can assign different levels of access to their users. The Salesforce Services also allow customers to assign access permissions based on the user's role. Salesforce's customer contracts restrict access by Salesforce's personnel as further outlined below in the section "Can Salesforce personnel access Personal Data in the Service".

Can Salesforce personnel access Personal Data in the 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 Salesforce Services?

Salesforce has policies and procedures in place to protect the security of the Salesforce Services. The security policies, procedures, and controls Salesforce makes available to customers are described in the Security, Privacy and Architecture documentation available here. Salesforce customers share responsibility for managing security. The Salesforce Services include a variety of security controls that a Salesforce 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 instances of the Salesforce Services.

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

Customers are responsible for using the Salesforce Services appropriately, including their processing of Customer Data on the Salesforce Services. Salesforce is responsible for providing the 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 Services?

The Salesforce Services allow customers to manage the Personal Data they maintain in the Salesforce Service, including in response to Data Subject requests. More detail about how to do so can be found in the Help Documentation. To the extent a customer needs Salesforce's assistance to respond to a Data Subject, Salesforce will provide assistance as described in Section 3 of 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 EU. As outlined in the preceding question, the Salesforce 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 three mechanisms to legally transfer personal data outside of the EU: (i) Binding Corporate Rules for Processors; (ii) the EU-US and Swiss-US Privacy Shield; and (iii) Standard Contractual Clauses. For more information about these transfer mechanisms and which Salesforce services will rely on which mechanism, please review the Salesforce's Data Processing Addendum.

Describe the Salesforce Services' information flow for personal data.

Salesforce provides a cloud-based Salesforce Platform, and customers can allow their users to access the Service from virtually anywhere with an Internet connection. Customers who build apps or websites on Salesforce may also receive app users or visitors from around the world. For these reasons, data may flow to or from Salesforce from global locations, depending on where the customer, its users, its app users and its website visitors are located.

In terms of data flows within the Salesforce Service:

- Personal Data about a Salesforce 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 Salesforce Services' storage facilities.

- Personal Data about a Salesforce customer's app Users or website visitors: Information about app users and website visitors is collected as the User or visitor performs activities on a Salesforce-hosted app or site. In this case, the information flows from the visitor's location to the Salesforce Services' storage facilities.

- Personal Data accessed by Salesforce personnel: 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 all Salesforce Services and includes an "order of precedence" clause in the event one mechanism is invalidated. Specifically, Salesforce offers Binding Corporate Rules for Processors, the EU-US and Swiss-US Privacy Shield certification, and the Standard Contractual Clauses for Sales Cloud, Service Cloud, Chatter, Community Cloud, and the Lightning Platform For the remaining Salesforce Services, Salesforce offers both Privacy Shield certification and Standard Contractual Clauses.

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

Personal Data is shared by a customer 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 customer expressly permits in writing.

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

Protections for Personal Data are described in the Salesforce customer's contract with Salesforce. Contractual documents containing protections for Personal Data include (1) a master subscription agreement between Salesforce and the customer; (2) Salesforce's Data Processing Addendum, 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 Salesforce customer, are described in the 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 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?

As described in the Security, Privacy, and Architecture Documentation, available here, the Salesforce Services encrypt data in transit and allow customers to encrypt some data at rest using Salesforce Shield.

VI. RETENTION/DISPOSAL OF INFORMATION

How long is Personal Data retained in the Salesforce Service?

Customers choose how long to retain Customer Data, including Personal Data, on the Salesforce 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 Customer Data, including 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 in the manner described in the Security, Privacy and Architecture Documentation, available here.

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 a customer if it receives a request to exercise rights related to the processing of Personal Data on the Salesforce Services (for which that customer is the Data Controller). The 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 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.