

This document provides more information about the privacy and security of the Marketing 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 Marketing Cloud

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 that takes effect on May 25, 2018. The GDPR expands 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 Fact Sheet, which defines a number of the terms used in this document.

Salesforce welcomes this law as an important step forward in streamlining data protection requirements across the European Union and as an opportunity for Salesforce to deepen our commitment to data protection. Similar to existing privacy laws, compliance with the GDPR requires a partnership between Salesforce and our customers in their use of our services. We’re committed to complying with the GDPR in providing services to our customers as a processor. And we’re committed to ensuring that our customers can continue to use our services while complying with GDPR. 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 Marketing Cloud Services¹, and to assist our customers in completing their data protection impact assessment for the Marketing Cloud Services. Capitalized terms not defined herein have the meaning set forth in Salesforce’s Master Subscription Agreement and/or Data Processing Addendum.

Security

The GDPR requires organizations to use appropriate technical and organizational security measures to protect Personal Data against unauthorized processing and accidental disclosure,

¹ This document covers the services branded as ExactTarget, Email Studio, Journey Builder, Mobile Studio, Advertising Studio, Advertising Audiences, Advertising Campaigns, Social.com, Social Studio and Predictive Intelligence (collectively, the “Marketing Cloud Services”). This document does not apply to other Salesforce services that may be associated with or integrate with the Marketing Cloud Services, such as DMP (formerly Krux), Pardot, or Radian6.

access, loss, destruction, or alteration. Salesforce Marketing Cloud has robust security and privacy programs in place that meet the highest standards in the industry. These programs enable Salesforce to comply with a variety of data protection laws and regulations applicable to Salesforce.

Architecture

The Marketing Cloud Services are operated in multi-tenant architecture that is designed to segregate and restrict customer data access based on business needs. This 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.

Security Controls

The Marketing Cloud 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, monitor the Marketing Cloud Services for unauthorized intrusions using network-based intrusion detection mechanisms. The Marketing Cloud 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 Salesforce's services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. Production data centers used to provide the Marketing Cloud 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 Marketing Cloud 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 the Marketing Cloud Services is available [here](#). Salesforce's information security control environment applicable to the Marketing Cloud Services has undergone an independent evaluation in the form of a SOC 2 report. Salesforce also has been awarded the [TRUSTe Certified seal](#) signifying that Salesforce's [Website Privacy Statement](#) and privacy practices related to the Marketing Cloud Services have been reviewed for compliance with [TRUSTe's Certification Standards](#). For the ExactTarget services, Salesforce has obtained HITRUST CSF Certification. A copy of Salesforce's HITRUST letter of certification is available upon request from your organization's Salesforce Account Executive. Additionally, the Marketing Cloud 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 Data Subjects a number of rights regarding how organizations handle their data. These rights require companies to have systems in place to respond to and effectively address Data Subjects' requests. For example, if an individual submits a request to have their Personal Data deleted and the relevant circumstances apply, companies must be equipped to find all the relevant Personal Data linked to that individual and delete it. The Marketing Cloud Services enable customers to process these requests by using tools within the products.

Basis of Data Processing and Right to Object: *In order to process Personal Data, organizations must have a lawful basis to process the data. Under the GDPR, there are six legal bases which organisations 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 to obtain appropriate consent from individuals. Customers are in the best position to determine the proper scope of consent required. The Marketing Cloud Services Help Documentation discusses the data being collected and how it is used.
- For more details about consent management in the Marketing Cloud 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 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.*

- All Marketing Cloud products will allow customers to provide portable copies of data to individuals.
- For more details about data portability in the Marketing Cloud Services, please see the [Help Documentation](#).

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

- Each Marketing Cloud product allows customers to modify data about individuals, such as changing email addresses, in response to individual requests.

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. Email Studio, Journey Builder, Automation Studio, Mobile Push and Mobile Connect. An individual can ask the Marketing Cloud customer (the data controller) to delete Personal Data through the lines of communication that the Marketing Cloud customer has established to accept such requests. Customers can honor the requests for the Marketing Cloud Services as follows:

- Customers have the ability to delete individuals’ Personal Data from their subscriber/contact lists within the Salesforce Marketing Cloud Contact Builder application. This deletion will occur within Marketing Cloud, and customers should also have a process to delete Customer Data from other products, including other Salesforce products like Sales Cloud.
- After a customer deletes Customer Data about an individual, the Customer Data will be placed in a suppression state for 14 days. During this time, the customer will not have access to this information and further processing ceases. The 14 day suppression state is used in case a customer needs to reverse or recover deleted Customer Data. At the end of 14 days, the Customer Data is marked for deletion.

B. Social Studio, Predictive Intelligence, Group Connect and Ad Studio.

- After receiving a deletion request from a customer or from a social network regarding deletion of an individual’s Personal Data, the Marketing Cloud Services’ deletion process will remove the Customer Data from active files so it cannot be used, and place it into a suppression state for 14 days. At the end of the 14 day period, the Customer Data is marked for deletion.
- In Predictive Intelligence, individuals have some control to adjust privacy settings to block future tags. Additionally, Marketing Cloud customers have the ability to stop sending tagged data (collected from web pixels) to individuals.

General Information:

- After a customer's contract with Salesforce terminates, Salesforce deletes Personal Data in the manner described in the Marketing Cloud Services Security, Privacy and Architecture Documentation, available [here](#).

- If a Salesforce customer needs assistance to delete Personal Data that it has submitted to the Marketing Cloud Services, Salesforce will provide assistance as described in its contract with the customer. Salesforce's current Data Processing Addendum is available [here](#).
- For more details about the right to erasure in the Marketing Cloud Services, please see the [Help Documentation](#).

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.*

Customers may respond to individuals' requests to restrict processing by following a similar process to data deletion, but rather than deleting the data, it will be moved to a non-processing file.

- In some situations, Customers may be able to respond to Restriction on Processing requests by placing Personal Data into a suppression state where it will no longer be visible and no further processing will occur. They can begin processing Personal Data about the individual again when they wish to lift the restriction.
- For more details about the right to restriction in the Marketing Cloud Services, please see the [Help Documentation](#).

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

II. OVERVIEW OF PERSONAL INFORMATION

Provide a general description of the Service.

The Marketing Cloud Services is a software-as-a-service solution. It is a hosted service that enables companies to develop and manage customizable digital marketing campaigns in order to develop personal relationships with consumers. The Marketing Cloud Services include Email Studio, a platform that allows for the creation of personalized email campaigns; Journey Builder,

a platform to manage customer lifecycles and interactions; Social Studio, a tool to listen and engage with social media platforms; Advertising Studio, a tool to connect digital marketing with CRM data; and Predictive Intelligence, a tool to measure and optimize consumer experiences.

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

Marketing Cloud customers choose what data to submit to, and collect with, the Marketing Cloud 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 consumers who are part of the customer's Marketing Cloud marketing campaigns (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?

Marketing Cloud 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 Advertising Studio, Predictive Intelligence, or Social Studio, but they may choose whether to submit health-related information to ExactTarget, 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?

As described in the Security, Privacy, and Architecture Documentation, available [here](#), Customers are contractually prohibited from submitting government-issued identification numbers or financial information to the Marketing Cloud. Customers are also contractually prohibited from submitting health-related information to Advertising Studio, Predictive Intelligence, or Social Studio. Customers can choose whether to submit health-related information to ExactTarget.

Where are the Data Subjects located?

This depends on how the Marketing Cloud customer uses the Marketing Cloud Service. For example, the locations of Data Subjects will depend on (1) what information the Marketing Cloud customer submits to the Service; and (2) where the Marketing Cloud customer's Users of the Service are located.

What is the general purpose for Processing the Personal Data?

The Salesforce Marketing Cloud Service is a hosted service that enables companies to develop and manage customizable, easy-to-use digital marketing campaigns. Thus, the Marketing Cloud

Service is typically used by customers to create and automate digital marketing campaigns and to analyze the impact of such campaigns. The Marketing Cloud customer, as the data controller, should determine its specific purpose for processing Personal Data on the Marketing Cloud Service. Salesforce processes Personal Data to offer the Marketing Cloud Service, under the terms agreed in its contract with the Marketing Cloud 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 Marketing Cloud customer's use case. However, such effects are not required or part of the expected 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 use. Thus, Salesforce does not directly communicate with its customers' consumers, and ensuring Data Subjects' awareness is the Marketing Cloud customer's responsibility. To the extent individuals 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 Marketing Cloud Service?

The Marketing Cloud Service's user interface allows customers to manage the Personal Data on the Marketing Cloud 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 Marketing Cloud Service managed?

Marketing Cloud customers can assign access to their Users. The 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 Service, to prevent or address technical or service problems, as compelled by law, or with the Marketing Cloud customer's written permission.

Who will manage security of the Marketing Cloud Services?

Salesforce has policies and procedures in place to protect the security of the Marketing Cloud Services. The security policies, procedures, and controls Salesforce makes available to Marketing Cloud customers are described in the Marketing Cloud Security, Privacy and

Architecture Documentation available [here](#). The Marketing Cloud customer shares responsibility for managing security. The Marketing Cloud Service includes a variety of security controls that the Marketing Cloud customer can configure; the 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 Marketing Cloud Services. Salesforce is responsible for providing the Marketing Cloud Services appropriately under its contract with its customers. Under that contract, Salesforce commits to using the data only to perform Salesforce's services, to prevent or address service or technical problems, as compelled by law, or as the customer expressly permits in writing.

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

The Marketing Cloud Service allows customers to manage the Personal Data they maintain in the Marketing Cloud 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](#).

Can Salesforce personnel access Personal Data on the Marketing Cloud 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 to provide the Marketing Cloud Service, to prevent or address technical or service problems, if compelled by law, or with the Marketing Cloud customer's written permission. The locations of Salesforce's Affiliates that employee personnel who may access Personal Data for these purposes is available in the Marketing Cloud Infrastructure & Sub-processors Documentation, 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 Marketing Cloud Services' storage locations are described in the Infrastructure and Sub-processors Documentation, available [here](#). In addition, Salesforce offers a mechanism to legally transfer personal data outside of the EU for the Marketing Cloud Services: the Standard Contractual Clauses. For more information about these transfer mechanisms and which Marketing Cloud Services will rely on which mechanism, please review the Salesforce [Privacy Statement](#).

Describe the Marketing Cloud Service's information flow for Personal Data.

The Marketing Cloud Service is a cloud-based platform, and customers can allow their Users to access the Marketing Cloud Service from virtually anywhere with an internet connection. Customers may also distribute marketing campaigns to individuals from around the world. For these reasons, data may flow to or from the Marketing Cloud to global locations, depending on where the customer, its licensed users, or its marketing campaign audiences are located.

In terms of data flows within the Service:

- Personal data about a Marketing Cloud 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 Marketing Cloud's storage facilities.
- Personal Data about a Marketing Cloud customer's marketing campaign audiences: Customers can enter information about their marketing campaign audiences. In this case, the information flows from the location of the person entering the data to the Marketing Cloud's storage facilities. Information is also collected as consumers interact with the customer's marketing campaign. In this case, the information flows from the consumer's location to the Marketing Cloud's 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—then 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 the Standard Contractual Clauses transfer mechanism for the Marketing Cloud services.

How (and with whom) will Personal Data be shared on the Marketing Cloud 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 Marketing Cloud customer expressly permits in writing.

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

Protections for Personal Data are described in the Marketing Cloud 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 Marketing Cloud customer, are described in the Marketing Cloud 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 Marketing Cloud 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?

Yes. As described in the Security, Privacy, and Architecture Documentation, available [here](#), the Service encrypts data in transit and allows customers to encrypt some data at rest.

Is security on the Service audited?

Yes. The Marketing Cloud Service is subject to various audits and certifications, which are described in the Security, Privacy, and Architecture Documentation, available [here](#).

VI. RETENTION/DISPOSAL OF INFORMATION

How long is Personal Data retained on the Marketing Cloud Service?

Customers choose how long to retain Personal Data on the Marketing Cloud 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 Marketing Cloud Service 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 its customer if it receives a request to exercise rights related to the processing of Personal Data on the Marketing Cloud Services (for which that customer is the Data Controller). The Marketing Cloud 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. And each of those attorneys is supported by a privacy attorney who specializes in data protection full-time. 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 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](#).