Data Protection and Privacy

Salesforce, Spring '21

'21

CONTENTS

DATA PROTECTION AND PRIVACY

Work your way toward complying with data protection and privacy regulations. Regardless of the regulations and policies with which you're complying, we give you guidance to help you evaluate the best way to meet your requirements.

Data protection and privacy regulations can require you and your company to keep individuals' personal data secure and private. We've listed some of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Personal Information Protection Act (PIPA), Japan
- Health Insurance Portability and Accountability Act (HIPAA), United States
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

Some regulations can include principles that are similar to one another. So we give you guidance on some of the common privacy principles.

Data Deletion: Delete Personal Data

Get guidance on deleting personal data as you comply with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how to best comply with the regulations that apply to your company.

Consent Management: Track Customer Consent and Honor Opt-Out Requests

Track your customers' approval for how your company interacts with them. Comply with customer requests to opt-out of sharing their personal information with third parties. To help you assess your compliance with data protection and privacy regulations, we give you examples of common customer requests. And we provide details to help you determine the best way to comply with the regulations that apply to your company.

Restriction of Processing: Restrict How to Process Personal Data

Prevent the processing of your customers' data when situations require you to do so. We give guidance on how to restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Data Access and Portability: Give Customers Their Data when They Want It

Export customer-related data when customers request it, so that you can work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider when you evaluate your compliance with the regulations that apply to you.

Customer 360 Privacy Center: Satisfy Customer Requests and Data Privacy Laws

Manage components of data privacy law, like the General Data Protection Regulation (GDPR), and fulfill customer requests on how their personally identifiable information (PII) is stored, deleted, and transferred. Salesforce Customer 360 Privacy Center is a managed package.

SEE ALSO:

Set Up Tracking and Storage of Certain Data Privacy Preferences

Store Customers' Data Privacy Preferences

Best Practices for Tracking Data Privacy

Data Deletion: Delete Personal Data

Get guidance on deleting personal data as you comply with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how to best comply with the regulations that apply to your company.

EDITIONS

Available in: All Editions

Data Deletion for Sales Cloud

Delete customers' personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that matter to you.

Data Deletion for Service Cloud

Delete customers' personal data collected in customer service cases and other support records to comply with data protection and privacy regulations. We give you examples of common customer requests, so you can determine a plan to comply with the regulations that matter to you.

Data Deletion for Experience Cloud Sites

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Data Deletion for the Salesforce Platform

You can delete customer data to comply with data protection and privacy regulations. These common requests and tips may help you determine how you might use Salesforce Platform features to work toward compliance with the regulations that apply to you.

Data Deletion for Marketing Cloud

Delete customers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Commerce Cloud

Delete personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Customer 360 Audiences

Delete shoppers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Financial Services Cloud

Delete customers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Health Cloud

Delete personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Pardot

Delete customers' personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data Deletion for Analytics

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Data Deletion for Quip

Sometimes it's necessary to delete a customer's personal data to comply with data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Data Deletion for Heroku

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

SEE ALSO:

Set Up Tracking and Storage of Certain Data Privacy Preferences

Store Customers' Data Privacy Preferences

Data Deletion for Sales Cloud

Delete customers' personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that matter to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

EDITIONS

Available in: All Editions

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and their related procedures.

Common Customer Request	Actions to Consider	Things to Consider
A client of ours moved out of the country, where we're not licensed to do business. So he wants us to purge his data.	Delete Records	Delete these records and fields for your client. - Contact

3

Common Customer Request	Actions to Consider	Things to Consider
		• Tasks • Calendar events • Any personal data in unindexed, free-text fields A way to search for personal data in unindexed fields is to export the data, and then search for the user's information. • Voicemail messages If you subscribe to Salesforce CPQ, consider deleting these records if they include your customer's personal data. • Quotes • Contracts • Orders • Invoices
My customer decided to do business with our competitor instead. She asked that we delete her personal data.	Delete Records	In addition to deleting your customer's contact or lead record, consider deleting: • Any personal data in unindexed, free-text fields A way to search for personal data in unindexed fields is to export all Salesforce data, and then search for the customer's information. • Voicemail messages • Calendar events And if you maintain a sandbox environment, refresh the environment afterward to remove that customer's data from it. If you use Salesforce Inbox, delete the contact from Salesforce Inbox, and from any other email system you use, such as Outlook or Gmail.
My customer died. The company he worked for requested that we remove him from our systems.	Delete Records	
A prospect of mine doesn't want us to store her email address and phone number.	Manage Leads	Delete any fields that store your prospect's email address and phone number. Start with the lead record. If you've created other records or activities related to your prospect, make sure that you remove her email address and phone number from those records too.

Common Customer Request	Actions to Consider	Things to Consider
		If you subscribe to Sales Cloud Einstein, deleting fields in lead records doesn't fully delete their content throughout the system. Consider deleting the lead record altogether, which deletes the record and its contents entirely. Then, create another lead record for your prospect, but without any email addresses and phone numbers.
A sales rep with my firm no longer works with us. She wants us to remove all her personal information from Salesforce.	Deactivate (Delete) Users	Consider deleting: • Any personal data in unindexed, free-text fields A way to search for personal data in unindexed fields is to export the data, and then search for the user's information. • Voicemail messages • Calendar events We store notifications and any personal data in them for 90 days. Keep in mind that editing personal data in user records doesn't change the content that appears in those notifications. Salesforce deletes notifications older than 90 days.
Sometimes, records related to the data that customers want us to delete links to workflows and other data that we want to retain. How do I avoid disrupting those workflows and creating other problems when I delete associated data?	Manage Contacts	Check with your company's legal counsel on options for making personal data in records obscure instead of deleting the records altogether. A way to make personal data obscure is to change details in the customer's contact record. So in the record, you'd delete data in all its fields, except for the Account and Last Name fields, which are required. And then for the Last Name field, you'd replace the customer's name with something like `Deleted Contact` or `Forgotten Contact`.
For Salesforce Inbox or Einstein Activity Capture, I'd like to delete email and events related to a specific customer.	• Delete Email and Events Logged by Einstein Activity Capture and Salesforce Inbox	If your customer doesn't want your company to keep any of her information, delete the customer's personal information from:

Common Customer Request	Actions to Consider	Things to Consider
	• Delete Records	• Salesforce Inbox • Any other email system you use, such as Outlook or Gmail • Any Salesforce records

Data Deletion for Service Cloud

Delete customers' personal data collected in customer service cases and other support records to comply with data protection and privacy regulations. We give you examples of common customer requests, so you can determine a plan to comply with the regulations that matter to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's not necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

EDITIONS

Available in: All Editions

Common Customer Request	Actions to Consider	Things to Consider
A customer in California is no longer associated with my company, and I want to delete her data.	Delete Records	In addition to deleting your customer's contact records and cases, consider deleting: • Any personal information in unindexed, free-text fields A way to search for personal information in unindexed fields is to export all Salesforce data, and then search for the customer's information. • Voicemail messages • Calendar events And if you maintain a sandbox environment, refresh the environment afterward so that you remove that customer's data from it. If you subscribe to Service Cloud Einstein, deleting fields in a record doesn't fully delete their content throughout the system. Consider deleting the record altogether, which deletes the record and its contents entirely. Then, create another record for your customer, but without the data you want deleted.

Common Customer Request	Actions to Consider	Things to Consider
A field service contractor, technician, or customer is no longer associated with my company, and I want to delete their data.	Get Field Service Data	To find and remove all references to a customer, partner, or employee, perform a global search in Salesforce. After you identify the records that reference the person, you can manually edit or delete the records as needed. 📝 Note: Global search isn't supported on text fields for these field service objects. • Address • Maintenance Plan • Product Item • Product Item Transaction • Time Sheet Entry • Work Order Line Item • Work Type But you can create custom reports to search these types of records. In Salesforce mobile apps, we store notifications and any personal data in them for 90 days. Keep in mind that editing personal data in user records doesn't change the content that appears in those notifications. Salesforce deletes notifications older than 90 days.
A customer with entitlement management is no longer associated with my company, and I want to delete their data.	Report on Entitlements	To find and remove all references to a customer, partner, or employee, perform a global search in Salesforce. After you identify the records that reference the person, you can manually edit or delete the records as needed. 📝 Note: Global search isn't supported on text fields for these entitlement management objects. • Entitlement • Service Contract But you can view records of these types in standard reports.

Common Customer Request	Actions to Consider	Things to Consider
A customer doesn't want their emails stored in a case.	Delete Records	Search and delete all email messages in a case.
Someone tweets my company Twitter handle, or posts to our Facebook page, and it creates a case. A contact and account are also created with their Twitter handle or Facebook account. She wants nothing to do with my company and asked that I delete her personal data.	Delete Records	To stop tweets and posts from automatically becoming cases, see Enable Moderation for Social Customer Service
Social Customer Service logs and error data include public profile data and content.	Monitor Debug Logs	Log data is deleted automatically after 30 days.
Sometimes, records related to the data that customers want us to delete links to workflows and other data that we want to retain. How do I avoid disrupting those workflows and creating other problems when I delete associated data?	Manage Contacts	Check with your company's legal counsel on options for making personal data in records obscure instead of deleting the records altogether. A way to make personal data obscure is to change details in the customer's contact record. So in the record, you'd delete data in all its fields, except for the Account and Last Name fields, which are required. And then for the Last Name field, you'd replace the customer's name with something like *Deleted Contact* or *Forgotten Contact.*

Data Deletion for Experience Cloud Sites

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

EDITIONS

Available in: All Editions

Common Customer Request	Actions to Consider	Things to Consider
My customer wants her Chatter feed activities, such as bookmarks, comments, and votes, removed from a site .	• Purge activities via User Activity, Purge and Missions User Activity, Purge. • Find and delete feed elements and comments via Connect REST API. • Maintain answer verifications and remove identifying information associated with them via Comment Capability, Verified.	• Will your customer agree to preserving Chatter feed activities in the site if her identifying information has been removed from them? • Is there any data that you have the right to retain?
My customer wants his files and content folders to be deleted.	Find and delete the content and content folders via SOAP API.	• Does the customer know how to make this request? • Is there any data that you have the right to retain? Review the terms of service with the customer. • Is the customer aware that his data is lost after it's deleted? • Are there other places in the site where your customer might have stored this data?
A customer wants us to remove her Chatter posts from a group.	• Find and delete feed elements and feed comments via Connect REST API. • Remove and change personally identifying information in the user's profile.	• Do you want to delete all the customer's posts? • Are you legally required to remove their posts? Review the terms of service with the customer.
My customer wants his identifying information removed from posts in a site.	• Remove and change personally identifying information in the user's profile. • Find and delete identifying content in posts via Connect REST API. • Find and delete feed tracked changes that contain personally identifying information via SOAP API.	• Consider other ways that this customer's personal information might be revealed in Chatter posts. • Search free-text fields for personally identifying information. • Search feed-tracked changes for personally identifying information.
My customer shared personal information in a Chatter post. How do we remove it?	• Feed Post and Comments Editing Overview • Find and delete posts via Connect REST API. • Update the post via SOAP API.	Does the user have permission to edit and delete posts?
My customer wants her information withheld from posts that she's flagged.	Find and delete records for the userId via SOAP API.	• Does the customer know how to make this request?

Common Customer Request	Actions to Consider	Things to Consider
		• Is there any data that you have the right to retain? Review the terms of service with the customer. • Is the customer aware that her data is lost after it's deleted? • Are there other places that this data is stored? Search and identify all the places where data might be stored.

My customer requests that his phone number and email address be removed from a Chatter message.	• A user with Manage Chatter Messages permission on the org can:
	
	  – Delete the message using the ChatterMessage sObject delete() method.
	
	  – Update the message body using the ChatterMessage sObject update() method, redacting the user's personal information.
	
	• In a community, the user requesting to be forgotten can flag the message. Then a user with Moderate Chatter Messages permission can use moderation to delete the flagged message.
		• Will your customer agree to preserving Chatter feed activities in the site if his identifying information has been removed from them?
		
		• Is there any data that you have the right to retain? Review the terms of service with the customer.
		
		• Is the customer aware that his data is lost after it's deleted?
		
		• Are there other places in the site where your customer might have stored this data? Search and identify all the places where data might be stored.

A customer asks that all her direct messages be removed.	• Find and delete feed elements and feed comments via Connect REST API. • In a community, the user can flag message posts or comments. Then a user with the Moderate Chatter Messages permission can use moderation to delete the flagged message.	• Will your customer agree to preserving Chatter feed activities in the site if her identifying information has been removed from them? • Is there any data that you have the right to retain? Review the terms of service with the customer. • Is the customer aware that her data is lost after it's deleted? • Are there other places in the site where your customer might have stored this data? Search and identify all the places where data might be stored.

Data Deletion for the Salesforce Platform

You can delete customer data to comply with data protection and privacy regulations. These common requests and tips may help you determine how you might use Salesforce Platform features to work toward compliance with the regulations that apply to you.

EDITIONS

Available in: All Editions

Many data protection and privacy regulations can require you and your company to delete customers' personal data when customers request it, or when it's no longer necessary for you to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them. You can also review considerations in other sections of this guide for Salesforce products that may use the Salesforce Platform.

Common Customer Request	Actions to Consider	Things to Consider
I've deleted sensitive data from my Production org, and now I want to delete that same data from my Full Copy Sandbox.	Refresh Your Sandbox	You can manually delete the data from your sandbox. If you choose to refresh your sandbox to duplicate your production org, check with your development teams first. Otherwise, work may be lost. Also remove the data from any data sets that you've created for development and testing.
An employee's left our company. I need remove their access to my org and delete all data associated with their login credentials.	• Passwords • Use Activations • User Sessions • Connected Apps	In addition to removing the user's org access, consider: • Expiring all passwords for that user • Revoking activation status • End usage tracking for Connected Apps • Remove user sessions Users and admins can also: • Disconnect the user's account from third-party accounts like Facebook • Change the user's password
I'm an ISV and I want to be sure that some data is removed from package versions I published.	To remove data from package versions, 1. Create a version of the package with the information removed 2. Use the existing push upgrade option to update all their customers to the new version of the package 3. To delete the original package version, file a ticket with Salesforce	
I want to find and delete data associated with a particular contact ID.	• Find information with reports • Build a flow that accepts a contact ID, finds all data associated with that contact ID, and deletes it. Learn how to build a flow.	Flows might not identify all the data to delete. After your flow finishes, consider running a report to identify any remaining information and then delete it.

Common Customer Request	Actions to Consider	Things to Consider
As a customer, I want to delete Event Monitoring data for a given user on request.	• Learn about deleting event logs.	Event Monitoring logs are treated as a single entity, which means you can't remove one single user's data from a log. Pinpoint the dates of the user's activity you want to delete. Then remove the logs in that date range. If you want to retain some data from these logs, you can make backups of logs before deleting them. Then, after you delete a log, remove specific users' data from your backups. Learn more about managing log files in the Event Monitoring Trailhead.
I'd like to delete a user's history programmatically. Can I do that?	• Delete custom big objects through Setup. • Use the deleteByExample( ) call to define an sObject that contains the fields and values you want to delete.	The deleteByExample( ) call can delete data in FieldHistoryArchive and custom big objects. Entire custom big objects can be deleted in Setup.
I want to let Community or Chatter users deactivate their own accounts on demand.	• Enable the User Self Deactivate feature.	Provide users with a mechanism to deactivate their accounts. You can create this mechanism declaratively or programmatically.
A customer referenced in my flows asked us to delete all information about them. How can I make sure I've deleted all references to information that could personally identify this customer?	• Manually remove the customer's records from the flow. • Use the $Flow.InterviewGuid variable to identify records that are saved when a flow is paused.	When a flow is paused, the flow interviews serialize the data that the flow references. The serialized data is saved to the database as a Paused Flow Interview record. After you find these records, you can delete them as you would any other record.
I want to delete a user and all the records associated with them.	• Manually or programmatically delete the values in non-required fields. • Anonymize data in required fields. For example, change an email address to "deleteduser@delete.myco.com." • Deactivate the User record by unchecking the Active field. • Delete any third-party account links used for authentication.	• When deleting information about employees, the employee should ask Salesforce Customer Support to re-enable the default email change verification settings. This setting prevents them from receiving verification emails if you anonymize their data in required fields. Customers don't receive verification emails, and don't need to contact Salesforce Customer Support. • Consider using Quick Actions to find information about customers like Customer Community or External Identity users. Go to the Contact record,

Common Customer Request	Actions to Consider	Things to Consider
		choose to disable the user through the Quick Action, find the disabled User record, and then manually delete remaining values.
I'm a developer, and I created an app that uses the Einstein Vision and Einstein Language APIs. A user of my app has requested that any personal data in the form of text or images be removed from any elements created by the API (such as examples, datasets, and models).	After you delete the relevant data, use the Einstein Vision and Einstein Language APIs to delete the dataset. Then create anew dataset from the source data and consider whether to retrain the dataset to create a model. • Delete a Dataset (Einstein Vision) • Delete a Dataset (Einstein Language) • Create a Dataset From a File Asynchronously (Einstein Vision) • Create a Dataset From a File Asynchronously (Einstein Language) • Train a Dataset (Einstein Vision) • Train a Dataset (Einstein Language)	
Some customers requested that we delete text or image data sent in for prediction.	Prediction data is deleted automatically within 48 hours.	
I want to delete orchestration instances that contain a customer's data.	To delete a specific instance associated with a particular customer, use the Salesforce IoT REST API to delete an instance associated with a unique identifier. If the customer's data is in all instances, you can delete all instances for an orchestration though the UI.	Deleting an orchestration deletes all its associated instances.
I want to delete my reaction to an Einstein Next Best Action recommendation.	To delete customer reactions, use Next Best Action, Reaction via Connect REST API.	

Data Deletion for Marketing Cloud

Delete customers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan

- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

📝 **Note:** Before you delete contact data from Marketing Cloud, export the list or data extension containing the deleted contact information for later review and regulatory compliance proof..

- Review any ENS subscriptions that contain engagement events.

Common Customer Request	Actions to Consider	Things to Consider

How do I delete specific contacts from my account?	• Export basic ID information from a list or data extensions before you begin any deletion process. Save this information in a location where you don't process data for future reference. This data helps ensure that you don't accidentally reimport deleted data.
	• Delete contacts in Contact Builder.
	• Use the delete calls for contacts in the Marketing Cloud REST API.
	• To delete data from Audience Studio, use these tools.
		• Ensure this functionality is available to your account by contacting your Marketing Cloud account representative. This feature applies to these apps:
		  – Advertising Studio
		  – Audience Builder
		  – Contact Builder
		  – Email Studio
		  – GroupConnect
		  – Journey Builder
		  – MobileConnect
		  – MobilePush
		  – Setup
		• If you delete subscriber information from Email Studio, that deletion applies only to the Email Studio Channel. To fully delete all contact information from Marketing Cloud, delete the contact record in Contact Builder using Contact Delete.
		• Contact Delete processes these values during the suppression and deletion phases:
		  – ContactKey or SubscriberKey
		  – ContactID or SubscriberID
		• If you add a contact with the same ContactKey or SubscriberKey but different ContactID or SubscriberID, you can introduce a deleted contact back into your system as a new entry with a new SubscriberID, and without previous statistics, clicks, or other personal data. We recommend retaining a list of

Common Customer Request	Actions to Consider	Things to Consider
		deleted ContactKey and SubscriberKey values to prevent this reintroduction into your system.
		• We recommend that Marketing Cloud Connect users delete information from Sales or Service clouds first, then delete information from Marketing Cloud. Use API calls to delete contact information from triggered send lists, Salesforce legacy lists, or Microsoft Dynamics CRM lists.
		• We recommend that Marketing Cloud users that use Audience Studio or Personalization Builder delete information from Marketing Cloud first, then Audience Studio or Personalization Builder.
		• Audience Builder removes deleted contacts during the regularly scheduled data load automation. This process creates an automation in Automation Studio with the name of `AB-<YourEID>-Contact Delete Program`. This step prevents the inclusion of those contacts in new audiences. Audience Builder also removes related usage data, data from sendable data extensions, and non-sendable data deleted manually from data extensions in Contact Builder at this time. Allow 24 hours for this deletion to fully process. You may see information from suppressed or deleted contacts in Audience Builder until the 24-hour deletion process fully completes.
		• Audience Builder users deleting contacts via the Contact Delete API must set the TrackChanges parameter to `true` to remove deletions upon the regularly scheduled data load automation.
		• Email Recommendations, Web Recommendations, and Web and Mobile Analytics use separate app and API interfaces to delete contact

Common Customer Request	Actions to Consider	Things to Consider
		information. One request to any product in this group affects all products. You can make Do Not Track and Do Not Profile preferences available in a customer profile center.
		• Einstein products accessed via the Marketing Cloud include Einstein Engagement Scoring, Send Time Optimization, and Einstein Engagement Frequency. When you terminate your contract or delete email and subscriber data for one or more subscribers, the data these features use is removed completely within the following 90 days. This data is excluded from analysis as soon as is feasible. You can make Do Not Track and Do Not Profile preferences available in a customer profile center.
		• For Twitter, Facebook and YouTube, Social Studio inherits deletion requests for public data from the applicable social network. For those social networks, data subjects must request deletion from the social networks, and Social Studio inherits those changes. Private data, such as direct messages, from these social networks can be deleted by customers directly in the Social Studio platform, although these deletions do not flow through to the applicable social networks. For deletion requests related to other social networks, contact your Marketing Cloud account representative.
		• To remove Interaction Studio data from sendable data extensions stored in Marketing Cloud, delete contacts in Contact Builder. You are responsible for removing any related information from other data sources, such as non-sendable data extensions, FTP uploads, and data extracts. You must also remove data from inside Interaction Studio.

Common Customer Request	Actions to Consider	Things to Consider
		• You are responsible for deleting applicable contact information from these sources: – FTP - Remove contact data from any stored files – Databases – Spreadsheets – Non-sendable data extensions - Use data retention policies or make the data extensions sendable to ensure that the Contact Delete process applies to those data extensions. – Send logs – Data emitted to your callback endpoint via Event Notification Services. • To implement data retention policies for existing data extensions, create a data extension with the appropriate policy. Next, import the data from the old data extension to the new data extension. You can then delete the old data extension. Update any automated processes using the old data extension with the new data extension. • Refrain from using deleted contacts as the subject of a test send to avoid accidental sends. • If you change a data extension to a sendable data extension after performing a Contact Delete request, the process does not include that data extension. • We delete contact keys from a contact record from other contact records as well, such as removing a parent's email address from a child's contact record. • Delete contact information from all accounts, including those accounts used for testing. • If a MobilePush data subject makes a data compliance request via Marketing Cloud, we send a silent push to the customer app to indicate the applicable

Common Customer Request	Actions to Consider	Things to Consider
		change. The MobilePush SDK also makes the customer app check in daily for data compliance changes. If Marketing Cloud sends the silent push and the device does not process it before the next check-in, the device may not comply with regulations until the check-in occurs. • After a Right to Be Forgotten request takes place, the data subject can opt in to further processing by deleting and reinstalling the customer app. • If the IP address is collected, when a contact is deleted, the IP address is deleted and cannot be used to track back to the contact.
How do I access my account data within 90 days of contract cancellation?	You can log in to your account for 90 days to export data via the user interface or the API.	• Marketing Cloud begins deletion of all customer information in an account 120 days after contract cancellation. • After 90 days, you cannot renew access to data. • A new account cannot access data from the previous account.
How do I stop all automations in my account within 90 days of contract cancellation?	• Stop an Automation Studio automation. • Stop a Journey Builder journey.	Stop all automations not used to export data or capture unsubscribes. This step prevents activities that could add new data to your account.
How do I unpublish all web-based materials in my account within 90 days of contract cancellation?	• Unpublish CloudPages. • Pause landing pages and microsites.	Do not unpublish or pause pages used to capture unsubscribe requests. These pages record the unsubscribe requests that you need to retain.
How do I stop all inbound and outbound activities not related to data export in my account within 90 days after contract cancellation?	• Stop all inbound data not used to capture unsubscribes, such as opt-in activities for email, SMS, and push messages. • Stop all outbound data transmission not used to export data, such as scheduled messaging sends or data exports. • Uninstall all third-party API integrations not used to export data or capture unsubscribes.	• API functionality depends on what you implemented for your account. Do not stop API functionality used to capture unsubscribe requests. • Marketing Cloud does not send or process triggered sends to suppressed or deleted contacts.

Common Customer Request	Actions to Consider	Things to Consider
	• Delete all custom API integrations not used to export data or capture unsubscribes.	
How do I delete a customer's personal information stored in a Datorama account?	Contact your Datorama account representative.	Tell your Datorama account representative to delete the relevant personal information.
How do I access my Datorama account data within 90 days of contract cancellation?	You have 14 days to export data yourself and 30 days after the cancellation date to contact your account manager.	• Datorama begins deletion of all customer information in an account 90 days after contract cancellation. • After 30 days, you cannot renew access to data. • A new account cannot access data from the previous account.

Data protection and privacy compliance can require you to encrypt all data during transit. We recommend taking these steps to ensure compliance.

• To help ensure TLS compliance, use the latest version of your browser and HTTPS addresses to connect to Marketing Cloud.

• Use OAuth access token authentication for REST and SOAP API calls.

• Follow our API security best practices.

• Use SSL certificates for all landing pages.

SEE ALSO:

Deliverable Name: DMP Documentation Portal

Manage Einstein Recommendations Customer Profile Data Privacy

Marketing Cloud Data Protection and Privacy Tools

Data Deletion for Commerce Cloud

Delete personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

EDITIONS

Available in: All Editions

Many data protection and privacy regulations can require you to delete shoppers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Personal Information Protection Act (PIPA), Japan

• Privacy Act, Australia

• Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have shoppers who want the data that you've collected on them deleted, or to opt-out of certain types of data sharing, review these common requests and the procedures related to them.

Common Shopper Request	Actions to Consider	Things to Consider
I want you to delete my data from the system after my account is deleted.	Delete all data associated with the customer, as shown in this table.	When you delete a customer, you delete certain associated data. See Deleting Customers. All other data deletion requires extra steps, as noted in this table. See Browser-Based Local Data Storage to consider whether to inform the shopper of any browser cookies that exist on their computer.
I want you to delete my order history.	Delete an order	Set up automatic order removal after a set number of days using the Order Retention setting. The shopper may need to keep certain data to fulfill their obligations under tax and other laws.
I want you to delete any guest baskets I create.	Set basket lifetime for unregistered guests	The system deletes guest baskets after 240 minutes by default.
I want you to delete any custom object containing my personal data.	Delete Custom Objects	The merchant creates and maintains custom objects that can contain personal data. Verify this using the Custom Object Editor in Business Manager.
I want you to delete my personal information from all gift certificates.	Remove customer data from gift certificates	Gift Certificates contain the email of a recipient. Either remove the recipient's email or delete the entire Gift Certificate. If you delete the entire Gift Certificate, consider how you will refund the remaining balance.
I want you to delete my personal information from redeemed coupons.	Delete email addresses from redeemed coupons	Remove email addresses from redeemed coupons using the Forget Email feature.
I want you to delete any lingering cookies or data objects.	Instruct customers to delete cookies and objects from their browsers.	The process to delete cookies and objects depends on the browser the shopper is using. Instruct shoppers to refer to the documentation for their browser.
One of my shoppers in California asked that we not sell her data to other companies.	Consider if a third-party integration, built by the customer or otherwise enabled in Commerce Cloud, is within the scope of the request and how you would respond.	Customers should consider if they need to build customizations to pass on the request to vendors.
I need to create a button on my e-commerce website to receive and honor consumer requests to not sell data to other companies.	Customers can create a button with a clear and conspicuous link on their website. It is the customer's responsibility to determine whether a button is needed. The customer and their implementation partner should build this button and any components to	Customers should consider, through customization, how they can track the request and their responses to them.

Common Shopper Request	Actions to Consider	Things to Consider
	address actions described in our Help & Training documentation.	
Commerce Cloud Order Management: I want you to delete my account and order records.	Learn about deleting Salesforce Order Management records	When one record is derived from another record, delete the derived record before the original record. This rule affects all summary objects. For example, when you delete an order, delete the corresponding order summary and any related change orders first. Deleting a record doesn't delete records that belong to it. For example, when you delete an order, delete its order items first. Also, remember to delete the order item summaries before the order items, because the summaries are derived from the underlying order item records.
I want you to delete information stored in my local browser sessions.	Browser-Based Local Data Storage	Commerce Cloud uses browser cookies and session storage objects to store and track information. This information can exist on machines with browsers running Commerce Cloud merchant applications, or with browsers accessing websites that run on Commerce Cloud.

Data Deletion for Customer 360 Audiences

Delete shoppers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have customers or users who want the data that you've collected on them deleted, review these common requests and their related procedures.

Common Customer Request	Actions to Consider	Things to Consider
A consumer wants my business to delete her personal data.	Manage Contacts	- Delete personal data from the customer's contact record.

Common Customer Request	Actions to Consider	Things to Consider
		• Delete the customer data from all Customer 360 Audience profiles. • Consider the time frame for deleting copies of the data from source systems. • If you've stored the customer's data in other areas of Salesforce, delete that data too. • If the customer data is stored in external systems, ask those data vendors to remove the data.
My customer has requested their personal data be deleted. I store customer data in Marketing Cloud and use the Marketing Cloud Connector to ingest data into Customer 360 Audiences.	Requesting Data Deletion	Submit data deletion requests first to Customer 360 Audiences. After 48 hours, submit data deletion requests to Marketing Cloud. This cadence prevents the reintroduction of Subscribers from Marketing Cloud to Customer 360 Audiences.

Data Deletion for Financial Services Cloud

Delete customers' personal data when it's necessary to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Personal Information Protection Act (PIPA), Japan

• Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

EDITIONS

Available in: **Professional**, **Enterprise**, and **Unlimited Editions**

Common Customer Request	Actions to Consider	Things to Consider
My customer wants their personal and household data deleted.	Delete Records Deactivate (Delete) Users	Remove the customer's personal data from any integrated source system and exclude from future data synchronizations, to prevent data from being repopulated into Financial Services Cloud. Delete customer records in ascending order of the following groups: Group 1

Common Customer Request	Actions to Consider	Things to Consider
		• Financial Holdings • Financial Account Transactions • Billing Statements • Cards • Revenue Group 2 • Financial Accounts • Assets & Liabilities • Opportunities • Leads and Referrals • Identification Documents • Financial Goals • Education • Employment • Groups (member of) • Tasks • Calendar Events Group 3 • Contact Group 4 • Account • Any personally identifiable information (PII) in unindexed, free-text fields To search for PII in unindexed fields, export the data, and then search for the customer's information. • Voicemail messages • Where the customer has access to a community, deactivate their user If you are running Einstein Analytics for Financial Services Cloud, run the Analytics data flow to remove the deleted records.
Before they were converted, a lead responded that they don't want to be contacted and they want their data deleted.	Delete Records	Delete the lead's record from the Lead/Leads and Referrals object along with any: • Tasks • Calendar Events

Common Customer Request	Actions to Consider	Things to Consider
		• Personally identifiable information (PII) in unindexed, free-text fields To search for PII in unindexed fields, export the data, and then search for the customer's information. • Voicemail messages If you are running Einstein Analytics for Financial Services Cloud, run the Analytics data flow to remove the deleted records.
My customer has requested that we remove a former joint account owner from an investment account and the account's associated data.	Delete Records	Remove personal data from any integrated source system, to prevent data from being repopulated into Financial Services Cloud. Remove the former joint account owner's details from the financial account record and then delete their records from Groups (for example, member of a household). If you are running Einstein Analytics for Financial Services Cloud, run the Analytics data flow to remove the deleted records.

Data Deletion for Health Cloud

Delete personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. These are some of the regulations that may apply to companies collecting and processing their customers' data:

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- California Consumer Privacy Act (CCPA), United States

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My patient wants all her personal data deleted from Health Cloud.	Delete Patient Data	Be sure to remove the patient's personal data from any integrated source systems and exclude it from any future data syncs, so it isn't reintegrated into Health Cloud.

Data Deletion for Pardot

Delete customers' personal data when it's necessary to comply with data protection and privacy regulations. We give you examples of common requests and things to consider. That way, you can determine a plan of action for complying with the regulations that apply to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- California Consumer Privacy Act (CCPA), United States
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A client of ours moved to a country where we're not licensed to do business. So he wants us to purge his data.	Deleting and Undeleting Prospects	Archive the prospect in the recycle bin, then permanently delete the prospect. To remove a prospect's data from Pardot Einstein, delete the prospect record in Pardot. Deleting the Pardot record triggers deletion of associated data in Pardot Einstein.
My customer decided to do business with our competitor. She asked that we delete her personal data.		
My customer died. The company he worked for requested that we remove him from our systems.		
A prospect of mine doesn't want us to store her email address and phone number.		
One of my prospects in California wants their consumer data deleted. How do I delete their data from a contact in Pardot Einstein?		
A sales rep with my firm no longer works with us. She wants us to remove all her personal information from Pardot.	Deleting Pardot Users	Delete the user.

Data Deletion for Analytics

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer left my company for a competitor's. She wants us to delete her personal data from reports and dashboards in our system.	• Delete Records • Set Up Historical Trend Reporting	After you delete the records related to the customer, refresh any reports that include the customer's personal data.
My customer left my company for a competitor's. She wants us to delete her personal data from the Einstein Analytics and Einstein Discovery content in our systems.	• Delete Records • Delete a Dataset • Edit, Share, or Delete a Dataset	• In Einstein Analytics, use replication to automate data deletion. See the next entry in this table. Replication isn't available for Einstein Discovery. • If you capture historical snapshots, delete the rows containing the customer's personal data in the snapshot.
I want to automate data deletion for Einstein Analytics.	Enable Data Sync and Connections	• When replication is enabled, deleting data from the Sales Cloud also deletes it within Einstein Analytics. • The timing for full deletion with replication depends on the replication interval. If the replication interval isn't short enough to meet your customer's requirements, you can manually refresh the data. • The replication process includes retention of a couple of backups. It can take two full intervals to pass before the data is removed from the system. • If you capture historical snapshots, delete the rows containing that customer's personal data in the snapshot.
A sales rep with my firm no longer works with us. She wants us to remove all her personal information from Salesforce.	Deactivate (Delete) Users	Consider deleting: • Templates • Shared folders • Stories (Einstein Discovery) • Any personal information in unindexed, free-text fields

Common Customer Request	Actions to Consider	Things to Consider
		A way to search for personal information in unindexed fields is to export the data, and then search for the user's information.

Data Deletion for Quip

Sometimes it's necessary to delete a customer's personal data to comply with data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants her personal information removed from her user profile on your Quip site.	Remove a customer's information from their Quip site through the Quip Business Portal.	Consult your company's legal counsel determine what you need to retain. Quip lets her delete her own documents and any of her comments. Use Quip search tools to find unstructured personal data in: • Direct messages • Chat rooms • Spreadsheets • Document conversations • Document contents
My customer wants to know all the places he can find his personal data in direct message threads, comment threads, chat rooms, documents, and spreadsheets.	In addition to Quip search tools, the Quip Root API locates data in all of your company's Quip documents. For details about the Root API, contact Quip Customer Support.	Quip lets users delete their own documents and any of his comments. Use Quip search tools to find unstructured personal data in: • Direct messages • Chat rooms • Spreadsheets • Document conversations

Common Customer Request	Actions to Consider	Things to Consider
		• Document contents If you've connected external data to Quip through a Live App or Live Data connection, take into account that deleting data from Quip doesn't delete data stored outside of Quip.
A customer wants to delete or modify unstructured data within documents and spreadsheets.	• Manually delete content in Quip. • Modify or delete data in Quip documents using the Quip Root API. For details about the Root API, contact Quip Customer Support.	Quip lets users delete their own documents and any of his comments. Your customer can use Quip search tools to find unstructured personal data in Quip documents and spreadsheets. Edit histories may contain your customer's personal data. You have options for deleting edit histories. • Tell your customer to delete the entire edit history of a document or spreadsheet by making a copy of it. Then, replace the document or spreadsheet with that copy. • Use the Quip Root API to permanently change or delete the edit history of a document or spreadsheet.
My customer wants his unstructured data deleted from direct message threads, comment threads, and chat rooms.	In addition to manually deleting content in Quip, you can use the Quip Root API to modify and delete data in your company's Quip direct message threads, comment threads, or chat rooms. For details about the Root API, contact Quip Customer Support.	Quip lets users delete their own documents and comments. Your customer can use Quip search tools to find unstructured personal data in conversations and in chat rooms.

Data Deletion for Heroku

Sometimes it's necessary to delete a customer's personal data to comply with various data protection and privacy regulations. We give you examples of common requests and things to consider, so you can comply with the regulations that apply to you.

Many data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep it. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

EDITIONS

Available in: All Editions

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A client of ours moved out of the country where we're not licensed to do business. So the client wants us to purge their data.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can design and develop application-layer functionality that allows your organization to fulfill data deletion requests from your application's end users.	
I've deleted sensitive data from my primary Heroku Postgres database and now I need to delete that same data from database backups.	The following backups of data stored in your organization's Heroku Postgres database might be created depending on the Heroku Postgres plan your organization has selected and the features your organization have utilized. Salesforce Heroku provides Heroku PGBackups to assist your organization in creating manual or scheduled logical backups of Heroku Postgres databases. The retention period for backups created using Heroku PGBackups is described in the documentation and depends on the Heroku Postgres plan selected. Customers can also initiate the deletion of completed backups at anytime using the command "heroku:pg:backups:destroy <BACKUP_ID>." (Note: you can generate a list of all completed backups for an application via the command "heroku pg:backups -a app_name.") For selected Heroku Postgres plans, your organization can fork a database. This creates a new database containing a snapshot of an existing database at the current point in time. You can also create a Follower database which replicates any changes performed on your primary Heroku Postgres database. Your organization can use the "heroku addons:destroy" command to initiate deletion of a primary, forked or follower Heroku Postgres database.	Salesforce Heroku provides access to the pg_dump PostgresSQL tool which allows your organization to create and manage your own logical Heroku Postgres backups and retention schedule. Salesforce Heroku also offers selected Heroku Postgres Continuous Protection (physical backups) for Heroku Postgres. The retention period depends on the plan selected and once the retention period is reached, the data deletion process is automatically initiated. Heroku Connect synchronizes data between your Salesforce Services org and a Heroku Postgres database. Therefore copy(ies) of your Heroku Postgres data might reside in your Salesforce Services org.

29

Common Customer Request	Actions to Consider	Things to Consider
I've deleted sensitive data from my Heroku Redis database and now I need to delete database snapshots.	Heroku Redis is an in-memory, key-value data store and is not meant for long-term data persistence. After your organization deletes data stored in Heroku Redis, it initiates the data deletion process for any Heroku Redis database snapshots that Heroku Services created.	Only selected Heroku Redis plans include persistence and High Availability options that result in database snapshots being created.
I would like to delete sensitive data from Heroku Kafka.	Heroku Kafka supports time-based retention and log compaction. When the retention window is reached, the data clean up and removal process is initiated. Customers can configure the time-based retention period for Heroku Kafka to a shorter period at anytime to hasten the initiation of the data cleanup and the removal process.	The Heroku Kafka retention period for time-based retention is configurable and depends on the Heroku Kafka plan selected as described in the documentation.
I want to delete logs for an application I've deployed on Heroku.	Heroku's Logplex is designed for collating and routing log messages, not for storage of log data on a longer term basis. It keeps a minimum number of lines of consolidated logs that expire after 1 week. Your organization can choose to drain logs to a drain service provided by a third-party add-on or implement your own log drain to gain additional control over your logs. Shield Private Spaces also includes the feature Private Space Logging which enables you to configure log capture at the space level instead of the app level. This feature allows your organization to forward all log events from applications and Heroku system services in the space to a single external log capture destination as described in the documentation.	If a third-party add-on is utilized to store logs, then your organization needs to work with the add-on provider to determine steps to minimize third-party add-ons from capturing your users' personal data. Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on. Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on. If the Shield Private Spaces feature Private Space Logging is utilized, then logs are not stored within Heroku Services and your organization would need to delete the logs from the location where the logs were sent.

Consent Management: Track Customer Consent and Honor Opt-Out Requests

Track your customers' approval for how your company interacts with them. Comply with customer requests to opt-out of sharing their personal information with third parties. To help you assess your compliance with data protection and privacy regulations, we give you examples of common customer requests. And we provide details to help you determine the best way to comply with the regulations that apply to your company.

EDITIONS

Available in: All Editions

Consent Management for Sales Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Service Cloud

Respect your customers' requests to limit types and hours of contact. And honor customer wishes when they opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Experience Cloud Sites

Honor your customer's request to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for the Salesforce Platform

Respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Marketing Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Commerce Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Customer 360 Audiences

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Financial Services Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Health Cloud

Respect your customers' wishes when they request only specific types or hours of contact or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Pardot

Honor and respect your customer's wishes when they request only specific forms of contact from your company or to opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Analytics

Track your customers' approval for how your company interacts with them and honor their requests to opt-out of certain types of data-sharing. To help you assess your compliance with various data protection and privacy regulations, we give you examples of common customer requests. And we provide details to help you determine the best way to comply with the regulations that apply to your company.

Consent Management for Quip

We can help you honor your customer's request to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Consent Management for Heroku

Honor your customers' wishes to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

SEE ALSO:

Set Up Tracking and Storage of Certain Data Privacy Preferences

Store Customers' Data Privacy Preferences

Consent Management for Sales Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

<div style="float:right">

EDITIONS

Available in: All Editions

</div>

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
Some of my prospects don't want to receive calls or email messages from my company. They specifically prohibit us from calling, sending email messages, and sending sales materials through the post.	- Manage Contacts - Manage Leads	Delete information in these fields for lead records. - Phone - Mobile - Email - Mailing Address And in those records, select these options. - Email Opt Out - Do Not Call If you don't see those options for leads and contacts, add them to lead and contact page layouts, or ask your admin for help.

Common Customer Request	Actions to Consider	Things to Consider
One of my customers asked that we don't track if and when she opens email from us.	Enable Email Tracking for Individuals Opening Email from Your Company	Turn off tracking for whether and when your customers open email that you send from Salesforce. Also ask your customer whether it's OK for you to send her email from your company. If it's not, open her contact, lead, or person account record and: • Delete the email address. • Select Email Opt Out.
My customer doesn't want his social profile image to appear on Salesforce records.	Hide Social Network Profiles on Accounts, Contacts, and Leads	Ask your customer whether he's OK with you tracking any of his social profile content. Learn about security and privacy for social profile content in Guidelines for Using Social Accounts, Contacts, and Leads.
One of my customers in California has requested that we not share her personal data.	Manage Contacts	If you shared your customer's personal data with other parties, ask them to delete her personal data. The customer's personal data might be stored in other locations, including other areas in Salesforce.
Some of our prospects and customers don't want to hear from my company, unless they specifically opt in.	• Manage Leads • Manage Contacts	When working with leads and contacts, select options for: • Email Opt Out • Do Not Call If you don't see those options for leads and contacts, add them to lead and contact page layouts, or ask your admin for help. Consider deleting phone numbers, email addresses, and mailing addresses, unless your customers give you consent to use them. And refrain from sending marketing and sales materials through the post.
I use Salesforce Inbox and want to exclude specific prospects and contacts from receiving mass email distributions from me.	• Manage Leads • Manage Contacts	
For Salesforce Inbox or Einstein Activity Capture, we decided to not receive read receipts when our customers open our email messages.	Disable Email Tracking for Inbox Users	Turning off read receipts prevents all your Salesforce users from receiving read receipts. If you don't disable read receipts for all users, individual users control whether to include a read receipt for email messages they send.
A prospect of mine doesn't want us to store her email address and phone number.	Manage Leads	Delete any fields that store your prospect's email address and phone number. Start with the lead record. If you've created other records or activities related to your

Common Customer Request	Actions to Consider	Things to Consider
		prospect, remove her email address and phone number from those records too.
A lead I'm pursuing is interested in our services, but she's in the process of moving out of state. She asked that we give her a couple months before we continue soliciting her.	Manage Leads	Don't send email, schedule meetings, or call those customers. Select these options in the lead or contact record. • Email Opt Out • Do Not Call If you don't see those options for leads and contacts, add them to lead and contact page layouts, or ask your admin for help. Also, set a reminder to contact your prospect at the time your customers specify.
I use Sales Cloud Einstein. My customer asked us to exclude his personal data from factoring into machine learning models. That's because he doesn't want us to generate predictions based on his personal data.	• Exclude People's Personal Data from Modeling and Predictions • Create Custom Fields	For any of the following objects, create a custom field using the type Checkbox, and give it the API name `AI_HasOptedOutProfiling__c`. • Account (applies to person accounts only) • Contact • Contact Role • Lead • Opportunity • Activity And if you're using Salesforce Inbox or Einstein Activity Capture, consider excluding email data from machine learning models. For details, see Exclude People's Personal Data from Modeling and Data Enrichment.
For Salesforce Inbox or Einstein Activity Capture, I want to exclude a specific customer's personal data from being used by other Salesforce features.	Exclude People's Personal Data from Modeling and Data Enrichment	When you exclude your customer's data from third-party data enrichment, his standard profile data still appears. When you exclude his data from modeling, we no longer show recommended connections based on conversations with him.

Consent Management for Service Cloud

Respect your customers' requests to limit types and hours of contact. And honor customer wishes when they opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
Some of my customers don't want to receive calls or email messages from my company.	Delete Records	Delete information in these fields for lead records. • Phone • Mobile • Email • Mailing address And in those records, select these options. • Email Opt Out • Do Not Call
My customer doesn't want his social profile image to appear on Salesforce records.	Hide Social Network Profiles on Accounts, Contacts, and Leads	Ask your customer whether he's OK with you tracking any of his social profile content. Learn about security and privacy for social profile content in Guidelines for Using Social Accounts, Contacts, and Leads.
A customer in California asked us not to share his personal data with other divisions and third parties.	Manage Contacts	It's possible that your company stored your customer's personal data in other areas of Salesforce. If you shared your customer's personal data with other parties, ask them to honor the request and delete the customer's personal data.
My customer doesn't want my company to contact her for any sales-related reasons, just customer service.	Delete Records	Ask your customer about which forms of communication she allows for customer

EDITIONS

Available in: All Editions

Common Customer Request	Actions to Consider	Things to Consider
She specifically prohibits us from calling, sending email messages, and sending sales materials through the post.		service purposes, and retain the information specific to those forms. Consider deleting information related to the ways in which she prohibits contact.
As a Field Service mobile app user, I want to control when Salesforce uses my mobile phone to track my location.	Track Service Resources with Geolocation	Admins can turn geolocation tracking on and off for all Field Service mobile app users, and exclude specific individuals from geolocation tracking. Individual mobile users can also turn off location tracking for the mobile app from their phone's operating system settings.
My Field Service customer doesn't want to provide signatures electronically.	Manage Service Reports	To make field technicians aware of the customer's request before they arrive, create a custom field on service appointments to identify customers that need hard copies of their service reports. See Create Service Report Templates.
I use Service Cloud Einstein. My customer asked us to exclude his personal data from factoring into machine learning models. That's because he doesn't want us to generate predictions based on his personal data.	• Exclude People's Personal Data from Modeling and Predictions • Create Custom Fields	Let service agents exclude a case from the predictive model. Add a custom field on the Case object using the type Checkbox, and give it the API name $AI\_HasOptedOutProfiling\_\_c$.
My customer in California wants all the information he provided in one or more of his cases so he can share it with a third party.	Export Data	Consider which available data format best suits your customer's needs. You can use Data Loader to download and share CSV files of a customer's data. If the customer no longer wants you to keep the personal data you've collected, delete it.

Consent Management for Experience Cloud Sites

Honor your customer's request to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

EDITIONS

Available in: All Editions

If you have customers or users who request specific methods of contact from your company, review this common request and the related procedures.

Common Customer Request	Actions to Consider	Things to Consider
My customer doesn't want to be part of a group he was added to.	Join or Leave Groups	Do your customers know how groups work and how to control how they receive notifications from them?
My customer wants to be able to control how often she gets Chatter notifications.	Update Your Email Notifications in Chatter	• Are there other ways you communicate with customers? Do customers have options for controlling how other communications are received? • Do your customers have access to email notification settings?
My customer wants to be notified when his email address is changed.	Edit Your Email Settings	• Are there other ways you communicate with customers? • Do customers have options for controlling how the communications are received?
My customer followed a topic and only wants updates on it once a week unless she's mentioned on it.	Update Your Email Notifications in Chatter	• Are there other ways you communicate with customers? • Do customers have options for controlling how the communications are received?

I want to track my customers' preferences for receiving marketing materials.	Store customers' data privacy preferences.	• How quickly must you act on your customers' requests? Would setting a schedule help you keep track of when to act?
		
		• How do you determine which customers you've set privacy preferences for?
		  – You can retrieve updates to data privacy records when you set an Apex trigger on the Individual object.
		  – Using the SOAP API, you can run a query for record updates based on the Individual object.

I want to track my customers' preferences for processing and deleting their data.	Store customers' data privacy preferences.	• How quickly must you act on your customers' requests? Would setting a schedule help you keep track of when to act?

Common Customer Request	Actions to Consider	Things to Consider

		• How do you determine which customers you've set privacy preferences for?
		  – You can retrieve updates to data privacy records when you set an Apex trigger on the Individual object.
		  – Using the SOAP API, you can run a query for record updates based on the Individual object.

My customer wants to delete a comment that they posted in the feed of a public-facing site.	• FeedItem • Review and Approve Posts and Comments in Your Experience Cloud Site	Review Salesforce.com's policies for deleting content on public-facing site pages.
If I'm using an internalsite, am I subject to the same compliance as I would be for a public-facing site?	Check out the standards and limitations of use for external and internal Experience Cloud sites.	• Does the site store information on other clouds? • Has the customer purchased Experience cloud along with other clouds?

Consent Management for the Salesforce Platform

Respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

EDITIONS

Available in: All Editions

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A customer has asked to not receive emails that I send using a flow. How do I prevent a flow from sending an email?	Edit the flow to remove the user's contact information.	Consider periodically reviewing your contacts' contact preferences to make sure that your flow includes only those contacts who wish to receive emails.

Common Customer Request	Actions to Consider	Things to Consider
A customer in California sent me an opt-out request so that we don't refer to or share her personal data.	Build a Flow	Build a flow that: • Accepts a contact ID. • Finds all data associated with that contact ID. • Deletes the data. If you connect to external sources, consider deleting the data from those sources. Keep in mind that flows don't necessarily identify all the data to delete. After your flow finishes, run a report to identify any remaining information, and then delete it.
I want to be able to track customers' preferences for receiving marketing solicitations. How can I do that?	Store customers' data privacy preferences.	Work with your legal team to understand how quickly you must act on your customers' requests. Keep in mind that the preferences you set simply help you track your customers' requests. And it's up to you and your company to determine a way for honoring those customers' requests. You can identify the customers for which you've set privacy preferences by either: • Retrieving updates to data privacy records when you set an Apex trigger on the Individual object. • Running queries for updates to records based on the Individual object using the SOAP API. Consider setting a schedule for these tasks based how quickly you must act on your customers' requests.
I want to be able to track customers' preferences regarding processing or deleting their data. How can I do that?	Store customers' data privacy preferences.	Work with your legal team to understand how quickly you must act on your customers' requests. Keep in mind that the preferences you set simply help you track your customers' requests. And it's up to you and your company to determine a way for honoring those customers' requests. You can identify the customers for which you've set privacy preferences by either: • Retrieving updates to data privacy records when you set an Apex trigger on the Individual object.

Common Customer Request	Actions to Consider	Things to Consider
		• Running queries for updates to records based on the Individual object using the SOAP API. Consider setting a schedule for these tasks based how quickly you must act on your customers' requests.

Consent Management for Marketing Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. Customers can also request that you restrict tracking and analytical processing using their data. These functions can occur when deciding what content to deliver to customers or using that data to predict future behavior. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Telephone Consumer Protection Act (TCPA), United States
- Canada's Anti-Spam Law (CASL)
- Personal Information Protection Act (PIPA), Japan

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
• Email Studio users need to obtain consent for contacts receiving marketing communications. • MobileConnect users need to obtain consent for contacts receiving marketing communications, including double opt-in best practices and compliance with local regulations. • MobilePush users need to obtain consent for contacts receiving push notifications. Consent is not required to send inbox or in-app messages to contacts. • GroupConnect users need to obtain consent for contacts receiving marketing communications.	• Use profile and preference center functionality for Email Studio to capture consent and opt-in confirmation for your marketing messaging activities. These consent mechanisms also govern access to email data used in Einstein Engagement Frequency and Send Time Optimization. • MobileConnect, MobilePush, and GroupConnect users should use your website or messages to notify subscribers of privacy changes and reestablish consent. • Review consent management information for Audience Studio.	• Collection of compliance requests takes place outside of Marketing Cloud functionality. Determine the best process for your business to receive and store this information as part of your data protection and privacy regulation review. • Make sure your consent language corresponds to your privacy notices and policies. Provide explicit information about the data you collect. • Consent must be specific, informed, and unambiguous. Collect positive consent and avoid automatically selected checkboxes.

Common Customer Request	Actions to Consider	Things to Consider
• Audience Studio users need to obtain consent for contacts receiving marketing communications.		• The process for obtaining consent regarding messaging to children is stricter. • Contacts must be able to withdraw consent at any time. • Contacts must freely give consent, and you cannot base usage of your website on provision of consent. • Consent to use data must be specific for each purpose for which you use data.
I do not want Marketing Cloud to track my messaging and online behavior.	• Create a mechanism for receiving a Do Not Track request, such as a preference center. • Use the DoNotTrack preference attribute to suppress subscriber-level events, such as opens, clicks, and replies. • This process does not affect messages or tracking sent before the Do Not Track request. • Review any ENS subscriptions that contain engagement events.	• This process permits continued sending to contacts with the DoNotTrack preference attribute enabled. • You cannot track related behavioral interactions. • This function applies only to Email Studio and as a preference attribute. • Messages sent to contacts with the DoNotTrack preference attribute enabled do not appear in tracking reports and can cause incomplete or inaccurate reporting. • The Do Not Track feature stops your account from receiving open and link tracking data for a data subject for any sends after the request date. Sends from before the request date continue to return this data. We plan to stop reception of this data for all sends in a future release. • Contact records receive a value for the DoNoTrack attribute upon creation of the record. Any import after that creation does not overwrite that value. Any change requires a specific update in Marketing Cloud or via an API call. • The Do Not Track process doesn't stop subscriber data events from emitting to your Event Notification Service Callback if you're subscribed to events that contain subscriber data. Events can be emitted from before and after the Do Not Track request if the subscriber continues to engage with Marketing

Common Customer Request	Actions to Consider	Things to Consider
		Cloud content with tracking. Users should carefully opt-in and understand the implications to using the ENS engagement events.
One of my customers in California asked me to delete her information. How do I delete their personal data from the contact record?	Contact Delete in Contact Builder	• Deleting a contact in MobilePush and MobileConnect also deletes opt-out preferences associated with the contact. • Identify whether you track this customer in other Salesforce Clouds, and consider removing his contact data from them.
What data fields do Marketing Cloud Einstein features process?	Learn about Marketing Cloud Einstein	Data sets vary by feature, but Marketing Cloud Einstein processes data as needed for generating outputs of any specific feature. For example, to generate recommendations, Send Time Optimization and Engagement Frequency features look at email engagement data.
How do opt-out and rights request tools in Marketing Cloud affect Marketing Cloud Einstein features?	Data Deletion for Marketing Cloud	Marketing Cloud Einstein features process a rolling 90-day window of data.
A customer in California requested that I restrict his information. If I restrict or delete that contact in Marketing Cloud, is his information also removed from Advertising Studio segments?	Data Deletion for Marketing Cloud	To fully address a contact's rights request, consider any actions to take on social network platforms for which you've sent audience segments.
My customer in California wants to know what information we disclose to social network partners when I transfer an audience segment from Advertising Studio. Where do I find this information?	Get Started with Advertising Audiences	Review social network partners' privacy statements and compliance tools, as well as customer's privacy statement. Advertising Studio sends data to Facebook and Twitter and presents information to the data subject. These social media services act as the data controller.
I have a customer using Social Studio. I've interacted with her on a social network, and she asked that we not sell her data to other companies.	Social Studio does not sell private customer data without customer consent. Check the policy of the social network on which the customer's data is used.	If you or your customer enabled third-party integrations with other vendors, ask those vendors to honor the customer's request. Keep in mind that your customer can have data in other areas of Salesforce and with other social networks. Consult those social networks for details on their privacy policies.

Common Customer Request	Actions to Consider	Things to Consider
I use Social Studio, and have had customers ask about my company's privacy policy. Do I have a way to account for how I'm using consumer information that I collect?	Consult with your company's counsel for updating your privacy policy, so that you comply with global privacy laws. Review the data collected by each Marketing Cloud product. Then, make sure that your privacy policy aligns with global privacy laws.	If you or your customer enabled third-party integrations with other vendors, decide whether to disclose data-sharing details about those integrations in your privacy policy. Keep in mind that your customer can have data in other areas of Salesforce and with other social networks. Review the full Marketing Cloud Consent Management Framework.
What data fields do you collect in Marketing Cloud for statistical data based on clicks and opens?	Review the column to the right for detailed information about what information is collected by Marketing Cloud application.	Some data that may be collected by click or open in Marketing Cloud for statistics includes: • IP Address • Country • Region • City • Postal Code • Latitude • Longitude • Metro Code • Area Code • Application used to click to open an email • The deivce's operating system used to open an email • Whether a mobile device is used to open an email

Marketing Cloud collects different information based on the apps you use.

App	Data Collected
Advertising Studio	Advertising Studio sends data to Facebook and Twitter and presents information to the data subject. These social media services act as the data controller.
Audience Studio	• Three email pixels contained in Audience Studio content capture the hashed email address, the subscriber or contact ID value, and media content. Audience Studio uses this data for audience creation or segmentation. • A web tracking pixel obtained during login to a web site identifies a person. This function treats each different browser as an independent login and identifier.

App	Data Collected
Email Studio	- An open pixel determines when an email recipient opens a Marketing Cloud email. Marketing Cloud uses this data for email job statistics and reporting. - Marketing Cloud uses link tracking to log information about which links the email recipient clicks. Marketing Cloud uses this link tracking data for email job statistics and reporting.
Marketing Cloud Einstein Platform	- Einstein imports email templates, standard data tables such as data views, some user agent data, and the members_ subscriber list. Email content is not imported. - Einstein imports personalization strings, but not the data called by those strings. - Einstein does not import custom object data or data stored in custom data extensions.
GroupConnect	The LINE messaging service acts as the data controller. Collect consent for messaging using the LINE service.
MobileConnect	MobileConnect does not collect this kind of behavioral information.
MobilePush	- MobilePush records the geographic location of a device when the customer mobile app is used. - MobilePush records a message receipt that reports back on the messages the data subject received through the customer mobile app. - MobilePush tracks how many times the customer mobile app is opened, how long it is used, and other app usage statistics. - Your app must use the latest version of the MobilePush SDK to implement Do Not Track functionality. - If a data subject makes a data compliance request via Marketing Cloud, we send a silent push to the customer app to indicate the applicable change. The SDK also makes the customer app check in daily for data compliance changes. If Marketing Cloud sends the silent push and the device does not process it before the next check-in, the device may not comply with regulations until then. - Mobile app developers can consult the Android and iOS data protection and privacy documents for MobilePush SDK.
Personalization Builder	- Web & Mobile Analytics records the sites from which web site users come. - Web Recommendations uses a web tracking pixel to track web site user behavior. This information only includes links to the web site user browsing the web site if that web site user logged into that site. Web Recommendations uses the data to provide more relevant recommendations for purchase. If the web site user does not log into the site, then the data is collected and returned anonymously. - Personalization Builder apps use an in-app interface to deal with Do Not Track and Do Not Profile requests from data subjects. This action prevents Marketing Cloud from collecting tracking or profiling information on a data subject. - You can make Do Not Track and Do Not Profile preferences available in a customer profile center.
Social Studio	Data subjects must use the privacy settings provided by the applicable social networks to manage the social media data that is shared with Salesforce through our integrations with those social networks. Social Studio does not provide customers with any cookies or other tracking technology. Any consents required in connection with a customer's use of cookies or other tracking technology through the customer's social media accounts are managed solely by the customer.

Data protection and privacy compliance can require you to encrypt all data during transit. We recommend taking these steps to ensure compliance.

- To help ensure TLS compliance, use the latest version of your browser and HTTPS addresses to connect to Marketing Cloud.
- Use OAuth access token authentication for REST and SOAP API calls.
- Follow our API security best practices.
- Use SSL certificates for all landing pages.

SEE ALSO:

Deliverable Name: DMP Documentation Portal

Do Not Track Script

Marketing Cloud Data Protection and Privacy Tools

Marketing Cloud Add Contact Preferences REST API Documentation

Marketing Cloud Add Contact Preferences by ID REST API Documentation

Marketing Cloud Get Contact Preferences by ID REST API Documentation

Marketing Cloud Get Contact Preferences by Key REST API Documentation

Marketing Cloud Search Contact Preferences by Reference Type REST API Documentation

Consent Management for Commerce Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

EDITIONS

Available in: All Editions

Track your shoppers' approval for how your company interacts with them. Data subjects have the right to consent to the use of their personal data and can object to the processing of their personal data with respect to receiving marketing communications, online tracking, and user profiling. To help you assess your compliance with various data protection and privacy regulations, we give you examples of common shopper requests. And we provide details to help you determine the best way to comply with the regulations that apply to your company. For instance, a shopper visits a website and doesn't want any of their information tracked while visiting the site.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have shoppers who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
I don't want your site to track my personal information for marketing or other purposes.	Set the Tracking site preference Programmatically override the site preference using the Script API	A new site preference, Tracking, lets you set default tracking behavior for each storefront.

Common Customer Request	Actions to Consider	Things to Consider
	Read about a sample consent tracking implementation in SGJC (SiteGenesis JavaScript Controllers)	If you want to override this behavior for an individual shopper, you can implement your own consent management solution by calling the `dw.system.Session.isTrackingAllowed()` and `dw.system.Session.setTrackingAllowed(boolean)` methods. Session cookies are used by default, so you might want to discuss them with your legal team.
I don't want your app to track my personal information for marketing or other purposes.	Determine shopper's tracking preference using the Shop API HTTP/HTTPS headers. Search for the OCAPI Global HTTP Headers topic.	Shop API resources let you set the HTTP(s) header DNT, which indicates whether personal information should be tracked.
I want to know which cookies your site uses to store information about me.	Review the local browser storage topic to understand the usage and lifespan of data stored locally. Inform the shopper of cookies that might be relevant to their usage.	Many cookies are automatically deleted at the end of each session, but some have longer lifespans. A system or browser crash can prevent deletion.

Consent Management for Customer 360 Audiences

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

EDITIONS

Available in: All Editions

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A consumer in California asked my business not to sell their data.	• Apply the Restriction of Processing flag to the individual profile that includes your customer's personal information. • For Unified Individuals, apply this flag to each individual linked profile.	Review your processing activities with your legal counsel to determine how regulations that matter to your company affect your business.
My customer has requested their personal data no longer be processed for marketing purposes. I store customer data in Customer 360 Audiences and other Salesforce platforms.	Requesting Restrict Processing	Submit Restrict processing requests to all the Salesforce clouds you use to store your customer's personal data.

Consent Management for Financial Services Cloud

Honor and respect your customers' wishes when they request only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to opt out of phone and email communications.	Manage Contacts	Delete information in these fields for customer records. • Phone • Mobile • Email And in those records, select these options. • Email Opt Out • Do Not Call
My customer wants to opt out of cross-selling.	Manage Contacts	Delete Lead and Opportunity records for the customer, along with any related Tasks and Calendar events. Add a note to the customer's record to indicate that they don't want to be part of future cross-selling.

Common Customer Request	Actions to Consider	Things to Consider
A consumer who lives in California asked us not to sell or transfer her personal or financial data to third parties.	• Set Up Tracking and Storage of Certain Data Privacy Preferences • Use the Consent API • Strengthen Your Data's Security with Shield Platform Encryption	Honor your customers' wishes when they request specific forms of contact from your company or opt-out of certain types of data-sharing. The data privacy fields help you track a wide range of opt-out and privacy preferences. To reduce the chances of inadvertently revealing sensitive information, encrypt fields that contain personal information using Shield Platform Encryption. If any third-party integrations are within the scope of the request, pass the request along to those vendors.
A consumer who lives in California withdrew his loan application, and asked us to delete his personal data.	• Set Up Tracking and Storage of Certain Data Privacy Preferences • Data Deletion for Financial Services Cloud • Data Access and Export for Financial Services Cloud	Honor your customers' wishes when they request restricting or deleting their personal data. Look for customer data in other records, including leads, accounts, and groups, such as households. To identify customers who previously asked your company to delete their data, Select Forget this Individual in data privacy records. Offer customers an exported copy of their data before your company deletes it. If any third-party integrations contain the customer's personal data, ask those vendors to delete it. That way, you prevent the data from repopulating into Financial Services Cloud.

Consent Management for Health Cloud

Respect your customers' wishes when they request only specific types or hours of contact or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

EDITIONS

Available in: All Editions

48

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A patient wishes to be contacted only by email, not by phone or any other channel.	Delete information in the **Phone** and **Mobile** fields for lead, account, and contact records. In those records, select **Do Not Call**.	Ask your patient about which forms of communication she allows for patient care purposes, and retain the information specific to those forms. Consider deleting information related to the ways in which she prohibits contact. Learn about security and privacy for social profile content in Guidelines for Using Social Accounts, Contacts, and Leads.
A participant in a drug trial wishes to stop participating.	Set an expiration date for the participant's consent.	You may not be able to delete some data, such as participant e-signatures, even when the consent that they certify is withdrawn. For example, participant data for some drug trials must be stored until a required retention period expires.

Consent Management for Pardot

Honor and respect your customer's wishes when they request only specific forms of contact from your company or to opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

EDITIONS

Available in: All Editions

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
Some of our prospects and customers don't want to hear from my company, unless they specifically opt in.	Set Up a Confirmed Opt-In Process	Use a confirmed opt-in process to have prospects explicitly opt in to communications.
Some of my prospects don't want to receive email messages from my company.	• Opt Out a Prospect • Email Preference Pages • Exclude Opted-Out Prospects from 1:1 Engage Emails	Manually opt the prospect out of Pardot marketing emails. Direct prospects to email preference center pages to let them manage their own email subscriptions. Configure Salesforce Engage to respect opt-out status on 1:1 messages.

Common Customer Request	Actions to Consider	Things to Consider
My prospect doesn't want their activity to be tracked when they interact with my marketing content.	Control Tracking Opt-In Preferences	Configure opt-in preferences for your account to let prospects opt out of tracking. Add disclosure statements to your Pardot forms and landing pages that indicate prospects are opting in to tracking by submitting their information.
A prospect is interested in our services, but is in the process of moving out of state. The prospect asked that we give them a couple months before we continue soliciting.	Deleting and Undeleting Prospects	Send the prospect to the recycle bin to suppress emails and activity tracking. Undelete the prospect to resume soliciting them.
One of my prospects in California asked that I not share their data with other companies or use it for marketing purposes.	• Deleting and Undeleting Prospects • Opt Out a Prospect • Email Preference Pages • Exclude Opted-Out Prospects from 1:1 Engage Emails	Archive the prospect data in the recycle bin and then delete the prospect. Manually opt out the prospect from Pardot marketing emails. Direct prospects to email preference center pages to let them manage their own email subscriptions. Configure Salesforce Engage to respect opt-out status on 1:1 messages.
How do I make sure a prospect's data isn't used in machine learning or predictions?	Exclude People's Personal Data from Modeling and Predictions on page 88	To exclude a Pardot prospect, associate them with a lead that's excluded using AI_HasOptedOutProfiling___c.

Consent Management for Analytics

Track your customers' approval for how your company interacts with them and honor their requests to opt-out of certain types of data-sharing. To help you assess your compliance with various data protection and privacy regulations, we give you examples of common customer requests. And we provide details to help you determine the best way to comply with the regulations that apply to your company.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Privacy Act, Australia

If your customers or users want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer doesn't want us to include her data in some of my reports and dashboards.	• Filter a Dashboard • Filter Reports by Values	After you define a filter related to the customer for a report, be sure to refresh the report.
My customer doesn't want us to make predictions or inferences about her, such as her loyalty to our company's products and services.	Edit, Share, or Delete a Dataset	When you create a new analysis, the analysis will no longer include the deleted data.
My customer doesn't want her personal data included in my company's analytics using Einstein Analytics.	• Delete Records • Add Row-Level Security with a Security Predicate	Security predicates can restrict access to data, but a copy of that customer's data remains in Einstein Analytics.
One of my customers in California is no longer associated with my company, and I want to delete their data from Einstein Prediction Builder.	Delete records containing that customer's personal data from Sales Cloud, Service Cloud, or Salesforce Platform.	When you delete a record in Sales Cloud, Service Cloud, or Salesforce Platform, associated personal data is automatically deleted from Einstein Prediction Builder.
My customer located in California doesn't want her personal data included in my company's analytics using Einstein Prediction Builder.	Create a segment excluding records associated with that customer.	Excluded records aren't used to build predictive models or predictions.

Consent Management for Quip

We can help you honor your customer's request to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Data protection and privacy regulations can require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review these common requests and the related procedures.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to be in control of which notifications she gets.	Manage Notifications in Quip	Customers can fine-tune their notification preferences. Direct your customers to the Quip documentation for managing notifications.

Common Customer Request	Actions to Consider	Things to Consider
My customer doesn't want others to see what she is viewing or editing in Quip.	Make a copy of the documents and place them in Private folders.	Site members can use Private folders to work on documents in privacy. Tell your customer to: 1. Copy the shared document to their Private folder. 2. Read and make edits to the copied document in the Private folder. 3. Copy any changes in the Private folder to the original shared document. Users can manage sharing of any particular document, spreadsheet, or chat room. They can share documents with their entire company, with a smaller team within their company, or with no one.
My customer in California sent us an opt-out request so that we don't refer to or share her personal data.	To locate personal data, use Quip search tools.	Delete any comments and documents that include your customer's personal data. Quip Search finds unstructured personal data in: • Documents and conversations • Direct messages • Chat rooms • Spreadsheets • Slides If you connect external data through a Quip Live App or live data connections, deleting personal data in Quip doesn't delete it from those external connections. If you need help with identifying references to personal data, contact Quip Support.

Consent Management for Heroku

Honor your customers' wishes to receive only specific forms of contact from your company or opt-out of certain types of data-sharing. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- California Consumer Privacy Act (CCPA), United States
- Canada's Anti-Spam Law (CASL)

EDITIONS

Available in: All Editions

If you have customers or users who request specific methods of contact from your company, review this common request and the related procedures.

Common Customer Request	Actions to Consider	Things to Consider
I want to be able to request and track our users' consent to store their personal data and marketing, data processing, and data deletion preferences.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can design and develop application-layer functionality that allows your organization to obtain and track consent and preferences for your application's end users.	Work with your legal team to design a consent management system that works for your specific customer needs.
I want to utilize third-party add-ons from the Heroku Elements Marketplace to store and/or manage our users' personal data.	Salesforce Heroku provides the ability for your organization to deploy third-party add-ons from the Heroku Elements Marketplace to extend and enhance capabilities of applications your organization deploys to Heroku Services.	Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on. Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on.
How do I minimize our users' personal data from being output to logs generated by applications our organization deploys to Heroku Services?	Salesforce Heroku aggregates logs from your application's running processes, system components, and backup services as described in the documentation into a single channel known as Heroku Logplex. Your organization can minimize transmission of sensitive data into the Heroku Logplex log stream by: • Turning off logging for your Heroku Postgres database by using the --block-logs option when creating the database. • Excluding such data in URLs or query strings submitted to web processes. • Not configuring application processes to print such data to stdout. Shield Private Spaces also includes the feature Private Space Logging which enables you to configure log capture at the space level instead of the app level. This feature allows your organization to forward all log events from applications and Heroku system services in the space to a single external log capture destination as described in the documentation.	If the Shield Private Spaces feature Private Space Logging is utilized, then logs are not stored within Heroku Services. If a third-party add-on is utilized to store logs, then your organization needs to work with the add-on provider to determine steps to minimize your users' personal data from being captured by the third-party add-on. Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on. Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on.

Common Customer Request	Actions to Consider	Things to Consider
A customer in California sent us an opt-out request so that we don't refer to or share her personal data.	Work with your developer on tracking customers' consent and deleting their personal data.	Consult your legal team about designing a consent management system. Develop application-layer functionality that fulfills consent management and data deletion requests from your applications.

Restriction of Processing: Restrict How to Process Personal Data

Prevent the processing of your customers' data when situations require you to do so. We give guidance on how to restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

EDITIONS

Available in: All Editions

Restrict Data Processing for Sales Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Service Cloud

When needed, prevent the processing of your customers' and employees' data in your customer service center. We give guidance to help you restrict forms of data processing to help comply with the laws that are important to your company.

Restrict Data Processing for Experience Cloud Sites

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

Restrict Data Processing for the Salesforce Platform

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Marketing Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Commerce Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Financial Services Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Health Cloud

When situations require you to do so, you can prevent the processing of your patients' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Pardot

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restriction of Processing for Analytics

Prevent the processing of your customers' data when situations require you to do so. We give guidance on how to restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Quip

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

Restrict Data Processing for Heroku

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

SEE ALSO:

Set Up Tracking and Storage of Certain Data Privacy Preferences

Store Customers' Data Privacy Preferences

Restrict Data Processing for Sales Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

EDITIONS

Available in: All Editions

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My company received a legal hold for certain customer records.	Export Data	Export the customer's data to retain it. You can also add notes for any other restrictions to processing until the legal hold is lifted. Restrictions can include the suspension of: - Sending email messages - Calling - Soliciting in general
My customer told me that the personal data we have on file for her is inaccurate. Because of those errors, she wants us to stop processing her data until we've verified the data's accuracy.	Export Data	Export the customer's data to retain it. Then, delete her data from Salesforce. Work with your customer to verify the data's accuracy. Then, get her approval to resume processing her data.
My customer stopped doing business with us. Although we no longer need his data,	Export Data	Export the customer's data to retain it. Then, delete his data from Salesforce.

Common Customer Request	Actions to Consider	Things to Consider
he asked that we keep it because he's involved in a legal proceeding that possibly needs the data.		
For Salesforce Inbox or Einstein Activity Capture, I'd like to prevent email and events related to a specific email address from appearing in the activity timeline.	• Exclude Emails and Events from Being Added to Salesforce for All Users • Delete Email and Events Logged by Einstein Activity Capture and Salesforce Inbox	Adding that email address to the excluded list prevents Salesforce from showing related activity in the activity timeline. But keep in mind that email and events remain in Salesforce. If you want to completely restrict processing: 1. Export the customer's data to retain it. 2. Delete the customer's activity from Salesforce Inbox. 3. Delete the customer's data in Salesforce.

Restrict Data Processing for Service Cloud

When needed, prevent the processing of your customers' and employees' data in your customer service center. We give guidance to help you restrict forms of data processing to help comply with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer filed a lawsuit against my company. It's our policy to stop processing his data until we reach a settlement.	• Export Data • Delete Records	Export the customer's data to retain it. You can also add notes for any other processing restrictions until you reach a settlement. Restrictions can include the suspension of: • Sending email messages • Calling • Soliciting in general
Union regulations prohibit me from tracking technicians with the Field Service mobile app.	Manage Data Integration Rules for Field Service	Admins can turn geolocation tracking on and off for all Field Service mobile app users, and exclude specific individuals from geolocation tracking with user profiles.

Restrict Data Processing for Experience Cloud Sites

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A site member doesn't want our processes to flag her as a Knowledgeable User about a topic.	Flag the individual as HasOptedOutProcessing via SOAP API.	Are there other places that this data is stored? Restrict processing on that data as well.
A site member doesn't want to surface as a Top User in a site.	Flag the individual as HasOptedOutProcessing via SOAP API.	Are there other places that this data is stored? Restrict processing on that data as well.

Restrict Data Processing for the Salesforce Platform

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Some laws and regulations can require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My company received a legal hold for certain customer records.	Export Data	Export the customer's data to retain it. You can also add notes for any other restrictions to processing until the legal hold is lifted.
My customer told me that the personal data we have on file for her is inaccurate. Because of those errors, she wants us to stop processing her data until we've verified the data's accuracy.	Export Data	Export the customer's data to retain it. Then, delete her data from Salesforce. Work with your customer to verify the data's accuracy. Then, get her approval to resume processing her data.

Common Customer Request	Actions to Consider	Things to Consider
My customer stopped doing business with us. Although we no longer need his data, he asked that we keep it because he's involved in a legal proceeding that possibly needs the data.	Export Data	Export the customer's data to retain it. Then, delete his data from Salesforce.

Restrict Data Processing for Marketing Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

> ✏️ Note: Before you restrict contact data from Marketing Cloud, export the list or data extension containing the restricted contact information for later review and regulatory compliance proof.

Common Customer Request	Actions to Consider	Things to Consider
How do I prevent Marketing Cloud activities from processing the information for a specific contact?	• If you manage contact information via our REST API, use the contact restriction routes to prevent processing of a specified contact. • Contact your Marketing Cloud account representative to restrict processing or remove restrictions for a contact. To delete a restricted contact, request the removal of a restriction first. • Export information before you restrict processing to ensure you can prove regulatory compliance. • Review any ENS subscriptions that contain engagement events.	• Stop processing to verify data accuracy for a contact during a specific time period. • Stop processing data because said processing is unlawful, but the contact wants to retain data anyway. • The data is no longer required for activities, but you must hold the data for legal claims or hold. • Contact objected to processing under their right to object. • Marketing Cloud does not send or process triggered sends to restricted contacts. • Einstein Web Recommendations, Einstein Email Recommendations, and Web & Mobile Analytics use separate app and API interfaces to delete contact information. One request to any product in this group affects all products.

Common Customer Request	Actions to Consider	Things to Consider
		• Refrain from using restricted contacts as the subject of a test send to avoid accidental sends. • This restriction removes information from sendable data extensions. • The Do Not Track process doesn't stop subscriber data events from emitting to your Event Notification Service Callback if you're subscribed to events that contain subscriber data. Events can be emitted from before and after the Do Not Track request if the subscriber continues to engage with Marketing Cloud content with tracking. Users should carefully opt-in and understand the implications to using the ENS engagement events.
How do I remove restrictions for a previously restricted contact?	Contact your Marketing Cloud account representative to remove restriction for a previously restricted contact.	Remove processing restrictions only when legally permissible.

If a data subject makes a data compliance request via Marketing Cloud for MobilePush, we send a silent push to the customer app to indicate the applicable change. The SDK also makes the customer app check in daily for data compliance changes. If Marketing Cloud sends the silent push and the device does not process it before the next check-in, the device may not comply with regulations until then. After a Restriction of Processing request takes place, the data subject can opt-in to further processing by deleting and reinstalling the customer app.

MobileConnect continues to process and honor opt-out requests even when a contact is in a Restriction of Processing state. The contact does not receive a message confirming the opt-out. This opt-out persists even after a contact leaves the Restriction of Processing state.

Data protection and privacy compliance can require you to encrypt all data during transit. We recommend taking these steps to ensure compliance.

• To help ensure TLS compliance, use the latest version of your browser and HTTPS addresses to connect to Marketing Cloud.

• Use OAuth access token authentication for REST and SOAP API calls.

• Follow our API security best practices.

• Use SSL certificates for all landing pages.

1

SEE ALSO:

Marketing Cloud Data Protection and Privacy Tools

Restrict Data Processing for Commerce Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
I want you to stop accessing or processing my personal data until we can resolve a dispute.	Export a copy of the shopper's data and maintain it in a secure and restricted location. Delete the shopper's personal data and associated orders from the Commerce Cloud system.	You cannot delete Shopper data when there are any associated open orders. Investigate any open orders and resolve them with the shopper. If such a shopper wants to delete their data, you can inform them that deleting all Commerce Cloud-related cookies from their browser will disassociate them from any data stored in Commerce Cloud.

Restrict Data Processing for Financial Services Cloud

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to freeze their account due to pending litigation.	Export Data Delete Records	Export the customer's data to retain it. You can also add notes for any other restrictions to processing until the legal hold is lifted. If you also delete the records, remove personal data from any integrated source system. This deletion prevents data from being repopulated into Financial Services Cloud. Restrictions can include the suspension of: • Sending email messages • Calling • Soliciting in general
A lead is interested in our services, but they're in the process of relocating. They asked that we wait a few months before we solicit them.	Manage Leads	Don't send email, schedule meetings, or call the lead. Select these options in the lead record. • Email Opt Out • Do Not Call And set a reminder to contact your lead at the time they specify.
My customer is out of the country and doesn't want us soliciting them until they return.	Manage Contacts	Don't send email, schedule meetings, or call the customer. Set a reminder to contact your customer at the time they specify.

Restrict Data Processing for Health Cloud

When situations require you to do so, you can prevent the processing of your patients' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Among the laws that apply to many companies collecting and processing their customers' data are:

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States
- California Consumer Privacy Act (CCPA), United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

EDITIONS

Available in: All Editions

Common Customer Request	Actions to Consider	Things to Consider
Patient wants the health or life science organization to refrain from any processing of their data until further notice.	• Mark the patient's affiliations "Not Active" • Export Data	When you mark a patient's affiliation "Not Active," Einstein Analytics for Health Cloud does not process the patient's data related to that affiliation. Restrictions on data processing can include suspending communications via Chatter, email, phone, or soliciting in general. You can also add notes for any other restrictions to processing until the hold is lifted. If you need to retain the customer's data, export it.

Restrict Data Processing for Pardot

When situations require you to do so, prevent the processing of your customers' data. We give guidance to help you restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My company received a legal hold for certain customer records. My customer stopped doing business with us. Although we no longer need their data, they asked that we keep it because they're involved in a legal proceeding that possibly needs the data.	• Export Prospects • Delete a Prospect	Export the prospect's data to retain it, then archive the prospect in the recycle bin. Consider that some activities will unarchive the prospect, see Remove a Prospect from the Pardot Recycle Bin. To prevent this, permanently delete the prospect, see Data Deletion for Pardot.
My customer told me that the personal data we have on file is inaccurate. Because of those errors, she wants us to stop processing her data until we've verified the data's accuracy.	• Export Prospects • Delete a Prospect	Export the prospect's data to retain it, then archive the prospect in the recycle bin. Work with your customer to verify the data's accuracy. Then, get their approval to resume processing their data. Remove the prospect from the recycle bin to resume processing. Consider that some activities will unarchive the prospect, see Remove a Prospect from the Pardot Recycle Bin. To prevent this, permanently delete the prospect, see Data Deletion for Pardot.

Restriction of Processing for Analytics

Prevent the processing of your customers' data when situations require you to do so. We give guidance on how to restrict forms of data processing. That way, you can work toward complying with the laws that are important to your company.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer stopped doing business with us. Although we no longer need his data, he asked that we keep it because he's involved in a legal proceeding that possibly needs the data.	• Export Data • Delete Records.	Export the customer's data to retain it. Then, delete his data from Salesforce.
My customer told me that the personal data we have on file for her is inaccurate. Because of those errors, she wants us to stop processing her data until we've verified the data's accuracy.		• Work with your customer to verify the accuracy of the data. Then get her approval to resume processing of her data.

Restrict Data Processing for Quip

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

Laws and regulations can require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A customer wants to restrict further processing of specific documents or content within documents.	• Remove other users from a document, so that only you can access it. • Export or print a document, and then delete that document from Quip. • Create a snapshot of specific data at a specific time using the Quip Root API. For details about the Root API, contact Quip Customer Support. Or, ask Salesforce Customer Support for help. • Ask your admin to set your site to read-only status.	Account for any integrations with third-party documents management and workflow automation solutions. If you've connected data to Quip through a Live App or Live Data connection, take into account that restricting the processing of a Quip document doesn't stop any processing outside of Quip.
A customer wants to restrict processing on her profile information.	• Disable particular users through the Quip Business Portal. • Set your site to read-only status.	If your Quip site uses single sign-on (SSO), consider that the SSO provider may maintain user information.
My customer wants to restrict processing of unstructured data in direct message threads, comment threads, and chat rooms.	• In chat rooms and direct message threads, export or print the conversations in question, and then delete them from Quip. • Create a snapshot of specific data at a specific time using the Quip Root API. Or, ask Salesforce Customer Support for help. • Set your site to read-only status.	Quip users can connect chat rooms to external data sources via bots.

Restrict Data Processing for Heroku

Some situations require you to prevent the processing of your customers' data. We give you actions to consider so that you can work toward complying with the laws that are important to your company.

Various laws and regulations require you and your company to sometimes restrict the processing of your customers' data. We've listed a few of the laws that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Federal Rules of Civil Procedure, United States

If you encounter situations that require you to restrict data processing for any of your customers, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
My customer stopped doing business with us. Although we no longer need the customer's data, we were asked to keep it because of a legal proceeding that possibly needs the data.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can design and develop application-layer functionality that allows your organization to implement restrictions on data processing. Customers might also consider leveraging the following features and functionality available in Heroku managed add-ons to assist them in addressing such requests from end users of applications deployed to Heroku Services. Heroku Postgres provides the following data export and copy features for selected Heroku Postgres plans. - Heroku Postgres Dataclips allow your organization to generate a URL that can be accessed to download selected data in various formats. - Database backups can be generated using Heroku PGBackups or your organization can leverage the pg_dump PostgresSQL tool to generate backups. - Heroku Connect can be used to synchronize Heroku Postgres data to an existing Salesforce Services org. - Create a database fork which creates a snapshot of an existing database at the current point-in-time. Heroku Redis is not meant for long-term data persistence. Your organization should store data you wish to persist in Heroku Postgres and leverage the Heroku Postgres data export capabilities described previously. Heroku Kafka includes support for Kafka Consumers that your organization can utilize to export data to Heroku Postgres or to external systems. Your organization can also request full copies of sensitive data submitted to Heroku Services by visiting Heroku Support.	Work with your legal team to understand the types of data processing requirements that apply to your business. Export the customer's data to retain it.

65

Common Customer Request	Actions to Consider	Things to Consider
My customer told me that the personal data we have on file is inaccurate. Because of those errors, the customer wants us to stop processing their data until we've verified the data's accuracy.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can design and develop application-layer functionality that allows your organization to meet data processing restrictions. For example, ceasing further processing of data for your application's end users until your organization has verified data accuracy and also for obtaining and tracking these end-users' approval to resume processing of their data.	For selected plans, data changes made to your primary Heroku Postgres databases can be configured to replicate to Follower databases. However, data changes are not propagated to completed backups created using Heroku PGBackups or the pg_dump PostgresSQL tool, or previously forked databases. Therefore, customers should consider tracking any data changes and propagating these changes to forked databases, when restoring database backups created using PGBackups or the pg_dump PostgresSQL tool, or when performing a Heroku Postgres Rollback. Are there other places that this data is stored? Restrict processing on that data as well and work with your customer to verify the data's accuracy. Then, get their approval to resume processing their data.

Data Access and Portability: Give Customers Their Data when They Want It

Export customer-related data when customers request it, so that you can work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider when you evaluate your compliance with the regulations that apply to you.

Data Access and Export for Sales Cloud

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Service Cloud

When requested, provide the data you've received from your customers on cases and work orders to comply with various data protection and privacy regulations.

Data Access and Export for Experience Cloud Sites

Your customers can request a copy of the data we received from them. To work toward complying with various data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for the Salesforce Platform

You can use the Salesforce Platform to help you honor your customers' requests to prepare or package their data. We give you examples of common customer requests and tips. Then you can decide how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Marketing Cloud

When your customers request it, prepare and pack up the data you've received from them to work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Commerce Cloud

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Customer 360 Audiences

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Financial Services Cloud

When your customers request it, prepare and pack up the data you've received from them to work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Health Cloud

Your customers can request a copy of the data received from them and stored in Health Cloud. To work toward complying with various data protection and privacy regulations, export the data and pack it up.

Data Access and Export for Pardot

When your customers request it, prepare and pack up the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Access and Export for Analytics

Export customer-related data when customers request it, so that you can work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider when you evaluate your compliance with the regulations that apply to you.

Data Access and Export for Quip

Your customers can request a copy of the data we received from them. To work toward complying with data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Data Portability for Heroku

Your customers can request a copy of the data we received from them. To work toward complying with various data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

SEE ALSO:

Set Up Tracking and Storage of Certain Data Privacy Preferences

Store Customers' Data Privacy Preferences

Data Access and Export for Sales Cloud

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

EDITIONS

Available in: All Editions

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
A contact on my account left the company and wants to take her information with her.	Export Data	Consider which available data format best suits your customer's or prospect's needs. And if that person no longer wants you to keep the personal data you've collected, you can delete it. See Delete Records. If you subscribe to Sales Cloud Einstein and want to export lead data, you can request data containing past versions. Just contact Salesforce Customer Support for help.
My prospect decided to not proceed with a potential deal with us. Instead, she's working with our competitor. She asked for the personal data we collected from her.	Export Data	Consider which available data format best suits your customer's or prospect's needs. And if that person no longer wants you to keep the personal data you've collected, you can delete it. See Delete Records.
We received a legal hold on certain customer records. And a court order requires us to provide the data that's relevant to a specific customer.	Export Data	When you export this customer's data: - Retain a copy for restriction of processing purposes. - Provide a copy for the court order.
For Salesforce Inbox or Einstein Activity Capture, I'd like to give customers access to email read receipts I received after they opened email from me.	Create a case with Salesforce Customer Support	After you create a case, you'll get access to the read receipts for all email messages on which the customers were senders or recipients. Then, you can then provide any of that information to your customers.
I use Salesforce Inbox. One of my users wants to see the feedback on Einstein email insights that she provided.	Create a case with Salesforce Customer Support	After you create a case, you'll get access to the feedback provided to Einstein email insights. Then, you can provide that information to your user.

Data Access and Export for Service Cloud

When requested, provide the data you've received from your customers on cases and work orders to comply with various data protection and privacy regulations.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to know how many cases she has filed with my company.	Export Data	Consider which available data format best suits your customer's needs.
My customer wants to know how many points of contact my company has for him.		And if that person no longer wants you to keep the personal data you've collected, you can delete it. See Delete Records.
My customer wants all information they've provided in a case, or all cases, to give to another company or third party.		You can use Data Loader to download and share CSV files of a customer's data. See Data Loader Guide. If you subscribe to Service Cloud Einstein and want to export case data, you can request data containing past versions. Just contact Salesforce Customer Support for help.

Data Access and Export for Experience Cloud Sites

Your customers can request a copy of the data we received from them. To work toward complying with various data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
My customer doesn't want to do business with us anymore and wants to take data regarding her activity with her.	• User Activity, Export • Missions User Activity, Export • When to Use Data Loader	• What data do you want to make portable? • What data do you want to provide customers? • Is there any data that you have the right to withhold from customers? • Does any data need to be redacted, such as third-party confidential information? • Review your terms of service with your customer.
My customer wants a copy of all his Chatter posts.	• Find and export feed elements and feed comments via Connect REST API. • When to Use Data Loader	• What data do you want to make portable? • What data do you want to provide customers? • Is there any data that you have the right to withhold from customers? • Does any data need to be redacted, such as third-party confidential information? • Review your terms of service with your customer.

Data Access and Export for the Salesforce Platform

You can use the Salesforce Platform to help you honor your customers' requests to prepare or package their data. We give you examples of common customer requests and tips. Then you can decide how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union
• Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests. You can also review considerations in other sections of this guide for Salesforce products that may use the Salesforce Platform.

Common Customer Request	Actions to Consider	Things to Consider
A customer has requested that I export all data associated with their account. When I	Apex Policies for Transaction Security Notifications	Some orgs have security policies in place to block unauthorized data export events over

Common Customer Request	Actions to Consider	Things to Consider
try to export this data, I get blocked. What gives?		a certain size. Consider editing the policy's Apex code to temporarily increase the limits on how much data you can export. Once you've finished your task, edit the policy to return it to its previous settings.
A customer wants to review the account information they've given to us, which we stored in attachments on their account.	Export Backup Data from Salesforce	Salesforce orgs can generate backup files of your data on a weekly basis. Consider exporting some data, such as attachments, from these backups.
A customer wants to export all the data they uploaded to Einstein Vision and Language Service.	• Get a Dataset (Einstein Vision) • Get a Dataset (Einstein Language) • Get All Examples (Einstein Vision) • Get All Examples (Einstein Language) • Get All Models (Einstein Vision) • Get All Models (Einstein Language)	You can access individual examples, datasets, and models using the API. If you need to export more data, contact Salesforce Customer Support.
A customer wants me to delete data associated with them. How can I get their information from an orchestration instance?	Use the API return instance data associated with a unique identifier. After you find this data, export it.	
Our admin has left our company and doesn't want their information associated with any Salesforce IoT orchestrations or contexts.	Orchestrations and contexts contain references to the users who created them. To find all the orchestrations or contexts created by a certain user, use the Salesforce IoT REST API. Manually look at the createdBy field for both orchestrations and contexts. To change the createdBy value, change or delete the userID.	
I want to export my reaction to an Einstein Next Best Action recommendation.	To export customer reactions, use Next Best Action, Reaction via Connect REST API.	

Data Access and Export for Marketing Cloud

When your customers request it, prepare and pack up the data you've received from them to work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Customer Contracts

If you have customers or users who want to take the data that you've received from them, review this common request.

Common Customer Request	Actions to Consider	Things to Consider
Which tools do I use to export data from Marketing Cloud to respond to a contact's data portability request?	• Use the Contact Data Portability report to create a report containing subscriber data related to a single contact. • Use data extracts in your Marketing Cloud account. This material includes only data from Email Studio. • If you need more help, request a copy of information regarding specific contacts by contacting your Marketing Cloud account representative. • To export data from Audience Studio, use these tools.	• Use the appropriate data extracts to create static CSV files containing contact information on your FTP server or via download. You can then open and filter these files to produce the appropriate contact information. • If you need a custom extract or report to comply with specific regulations, such as GDPR, specify that need when you request the service. You are responsible for maintaining regulatory compliance for the data in your account. • Marketing Cloud reports and extracts do not process or extract information from deleted or restricted contacts.

Data protection and privacy compliance can require you to encrypt all data during transit. We recommend taking these steps to ensure compliance.

• To help ensure TLS compliance, use the latest version of your browser and HTTPS addresses to connect to Marketing Cloud.

• Use OAuth access token authentication for REST and SOAP API calls.

• Follow our API security best practices.

• Use SSL certificates for all landing pages.

SEE ALSO:

Deliverable Name: DMP Documentation Portal

Marketing Cloud Data Protection and Privacy Tools

Data Access and Export for Commerce Cloud

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

EDITIONS

Available in: All Editions

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Personal Information Protection Act (PIPA), Japan

• Privacy Act, Australia

• Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have shoppers who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
I want to download all of my data from your site.	Read about a sample data download implementation in SGJC (SiteGenesis JavaScript Controllers)	Determine what data the shopper is entitled to collect, how to format the data, and how to provide this capability to the shopper.
I would like a copy of my personal data that you are storing, but you don't provide a self-service option.	Export a snapshot of the shopper's data	Snapshots are in a technical format (JSON, XML) and can include several different types of data. Consider what you share and how to provide it. Determine what data the shopper is entitled to collect.

Data Access and Export for Customer 360 Audiences

When your customers request it, give them access to the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Personal Information Protection Act (PIPA), Japan
- Privacy Act, Australia
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
A consumer asked for a copy of their personal data. How do I process this request in Customer 360 Audiences?	Ask your API pro to: • Retrieve the party ID for each email address. • Export data for each associated party ID.	• Make this request for each Customer 360 Audience profile. • If multiple individual profiles link to a Unified Individual, request a copy for each profile. • If the customer data is stored in source or external systems, request that those vendors export the data.
My customer has requested a copy of all their personal data in my possession. I store customer data in Customer 360 Audiences and other Salesforce platforms.	Requesting Data Access and Export	Submit Data access requests to all the Salesforce clouds you use to store your customer's personal data.

Data Access and Export for Financial Services Cloud

When your customers request it, prepare and pack up the data you've received from them to work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to move an investment account to another institution and take the associated personal data with them.	Export Data Create a Report	Consider which data format best suits your customer's needs. You can obtain data from reports as follows: • Individual customer details can be obtained using a standard report on Account and Contact objects. • Household details can be obtained using a custom report created on the Account Contact Relationship object. • For business and personal relationships, create separate reports on the Account-Account Relationship and Contact-Contact Relationship objects. • Activities can be obtained using a standard report. • Financial Accounts can be pulled directly from Joint Owner or Primary Owner. • Customer Alerts can be pulled from Alerts. • Beneficiaries can be obtained from a standard report using Financial Account Role. • For other financial services data, use the standard reports. And if the customer no longer wants you to keep the personal data you've collected, you can delete it. See Data Deletion for Financial Services Cloud

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to review all account information (such as Financial Account Roles) on an annual basis. My customer wants to review their assets and liabilities.	Export Data Create a Report	Consider which data format best suits your customer's needs. You can obtain data from reports as follows: • Individual customer details can be obtained using a standard report on Account and Contact objects. • Household details can be obtained using a custom report created on the Account Contact Relationship object. • For business and personal relationships, create separate reports on the Account-Account Relationship and Contact-Contact Relationship objects. • Activities can be obtained using a standard report. • Financial Accounts can be pulled directly from Joint Owner or Primary Owner. • Customer Alerts can be pulled from Alerts. • Beneficiaries can be obtained from a standard report using Financial Account Role. • Assets and Liabilities can be obtained using a standard report. • For other financial services data, use the standard reports.
A lead decided to not open an account with us. They have asked for the personal data we collected from them.	Export Data Create a Report	Consider which data format best suits your lead's needs. You can obtain data on the lead using a standard report. And if your lead no longer wants you to keep the personal data you've collected, you can delete it. See Data Deletion for Financial Services Cloud

Data Access and Export for Health Cloud

Your customers can request a copy of the data received from them and stored in Health Cloud. To work toward complying with various data protection and privacy regulations, export the data and pack it up.

EDITIONS

Available in: All Editions

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts
- California Consumer Privacy Act (CCPA), United States

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
My patient wants to move all her data to another health care provider and leave no record with the old one.	- Create reports - Export Data - Delete Patient Data - Retrieve, export, and delete the NetworkActivityAudit records for the patient	Consider which data format best suits your patient's needs. You can obtain data from reports: - Account details can be obtained using a standard report. - Household details can be obtained using a custom report created on the Account Contact Relationship object. - For business and personal relationships, create separate reports on the Account-Account Relationship and Contact-Contact Relationship objects. - Cases, Activities, and Users can be obtained using a standard report. - Many managed custom objects, such as EHR objects, Candidate Patient, Provider, Program Patient Affiliation, Program Patient Summary, Problem, and Case, can be exported via standard reports.

Data Access and Export for Pardot

When your customers request it, prepare and pack up the data you've received from them to work toward complying with data protection and privacy regulations. We give you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
A contact on my account left the company and wants to take her information with her.	Export Prospects	Use the Pardot API or a CSV export. Consider archiving the prospect in the recycle bin, then contacting support to permanently delete the prospect.

Common Customer Request	Actions to Consider	Things to Consider
My prospect decided to not proceed with a potential deal with us. Instead, she's working with our competitor. She asked for the personal data we collected from her.		
We received a legal hold on certain customer records. And a court order requires us to provide the data that's relevant to a specific customer.	Export Prospects	When you export this customer's data: • Retain a copy for restriction of processing purposes. • Provide a copy for the court order.

Data Access and Export for Analytics

Export customer-related data when customers request it, so that you can work toward complying with various data protection and privacy regulations. We give you examples of common customer requests and things to consider when you evaluate your compliance with the regulations that apply to you.

Data protection and privacy regulations can require you to delete customers' personal data when customers request it, or when it's no longer necessary to keep. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

• General Data Protection Regulation (GDPR), European Union

• Personal Information Protection Act (PIPA), Japan

• Privacy Act, Australia

If you have customers or users who want the data that you've collected on them deleted, review these common requests and the procedures related to them.

Common Customer Request	Actions to Consider	Things to Consider
A customer is moving to a competing product and wants to port their dashboards and report data.	Export Data	• Export any reports containing the customer's data. • Dashboard charts aren't available for export, but you can use the Save As function to save a static image of a dashboard component.
A customer is moving to a competing product and wants to port their Einstein Analytics data.	• Export Data • Enable Downloading Data from Tableau CRM	• Filter to isolate the data related to the customer before downloading. • Download an image of the analysis of the customer's data.
A customer is moving to a competing product and wants to port their Einstein Discovery data.	• Export Data • Export and Share Insights	• Export an Einstein Analytics dataset associated with any story.

Common Customer Request	Actions to Consider	Things to Consider
		• Export snapshots of story insights to Quip. • Story settings and Einstein Discovery models aren't available for export.

Data Access and Export for Quip

Your customers can request a copy of the data we received from them. To work toward complying with data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers access and take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to export a list of his contacts on Quip.	• If you have admin rights, retrieve a list of contacts using the Quip API GET command. • Visit your Business Portal to look up a customer's data. Then, copy and paste that data into a format that you can share with your customer.	Consider reviewing the exported data first before you share it with your customer. That way, you can ensure that you don't share data not intended for that customer.
My customer wants to see a full record of her activity in Quip.	Request a record of the customer's activity from Quip Customer Support.	Determine if there is confidential content, third-party content, or personal data of other users in the material that you're sharing. You may want to redact it first.
My customer wants to export a copy of a spreadsheet or document.	• Use the "Export" command in the Document and Spreadsheet menus. • Cut and paste the spreadsheet or document from Quip into another application. • Print content using the "Print" command in the Document and Spreadsheet menus. • Export the content using the Quip Automation API with a personal access token.	If your customers use the "Export" command, they can then save the content in these formats. • PDF • Microsoft Word • HTML • Markdown • LaTeX

Common Customer Request	Actions to Consider	Things to Consider
My customer wants to get a copy of the information in her user profile.	Visit your Business Portal to look up your customer's data. Then, copy and paste that data into a format that you can share with your customer.	Consider reviewing the data first before you share it with your customer. That way, you can ensure that you don't share data not intended for her.

Data Portability for Heroku

Your customers can request a copy of the data we received from them. To work toward complying with various data protection and privacy regulations, export the data and pack it up. We've given you examples of common customer requests and things to consider. That way, you can determine how best to work toward complying with the regulations that apply to your company.

Some laws require you and your company to let customers take their data with them. We've listed a few of the obligations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Customer Contracts

If you have customers or users who want to take the data that you've received from them, review these common requests. We've provided links to the procedures related to those requests.

Common Customer Request	Actions to Consider	Things to Consider
A user wants to review or export the account information they've submitted to our application.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can develop application-layer functionality that allows your application's end users to access, review, and export data submitted to your application. In addition to developing application-layer functionality, your organization might consider leveraging the following data export features available for Heroku managed add-ons. Heroku Postgres provides the following data export features for selected Heroku Postgres plans. - Heroku Postgres Dataclips allow your organization to generate a URL that can be accessed to download selected data in various formats. - Database backups can be generated using Heroku PGBackups and/or your organization can leverage the pg_dump PostgresSQL tool to generate backups.	- What data do you want to make portable and what data format best suits your customer's needs? - What data do you want to provide customers? - Is there any data that you have the right to withhold from customers? - Does any data need to be redacted, such as third-party confidential information? - Review your terms of service with your customer.

Common Customer Request	Actions to Consider	Things to Consider
	• Heroku Connect can be used to synchronize Heroku Postgres data to an existing Salesforce Services org. Heroku Redis is not intended for long-term data persistence. Your organization should store data you wish to persist in Heroku Postgres and leverage the Heroku Postgres data export capabilities described previously. Heroku Kafka includes support for Kafka Consumers that your organization can utilize to export data to Heroku Postgres or to external systems. Your organization can also request full copies of sensitive data submitted to Heroku Services by visiting Heroku Support.	
How do I export logs generated by applications our organization deploys to Heroku Services that might contain our users' personal data?	Heroku's Logplex is designed for collating and routing log messages, not for storage of log data on a longer term basis. Logplex keeps a minimum number of lines of consolidated logs that expire after 1 week. Your organization can choose to drain logs to a drain service provided by a third-party add-on or implement your own log drain to gain additional control over your logs. Shield Private Spaces also includes the feature Private Space Logging which enables you to configure log capture at the space level instead of the app level. This feature allows your organization to forward all log events from applications and Heroku system services in the space to a single external log capture destination as described in the documentation.	Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on. Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on. If the Shield Private Spaces feature Private Space Logging is utilized, then logs are not stored within Heroku Services.

Customer 360 Privacy Center: Satisfy Customer Requests and Data Privacy Laws

Manage components of data privacy law, like the General Data Protection Regulation (GDPR), and fulfill customer requests on how their personally identifiable information (PII) is stored, deleted, and transferred. Salesforce Customer 360 Privacy Center is a managed package.

Requires the Salesforce Customer 360 Privacy Center add-on subscription.

To manage how long your org keeps customer data, create right to be forgotten and data retention policies with the Data Deletion, Retention, and Archiving feature. Right to be Forgotten policies automate how and when customer PII is deleted from your org. Data retention policies automate how PII is stored and archived in your org, with options to make data anonymous at the field level. Use the Data Subject Access Request feature to create portability policies. Portability policies automate how a copy of PII data is sent to your customer. After you create a portability policy, execute the Portability API to compile and securely send a copy of all PII from your org to your customer.
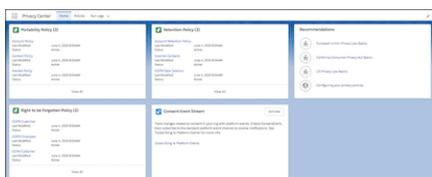
To get started, contact Salesforce Customer Support to enable Customer 360 Privacy Center. Then open the Customer 360 Privacy Center dashboard from the App Launcher.

Provision Heroku Resources to Use Privacy Center

Salesforce Customer 360 Privacy Center uses Heroku for data processing and storage. The Privacy Center license includes add-on credits that you use to provision Heroku resources for the Data Retention feature.

Create Data Deletion, Retention, and Archiving Policies

Satisfy your customers' right to be forgotten requests and manage data retention in your org by creating policies that delete or make personally identifiable information (PII) anonymous at record or field levels. Use this feature to retain or archive data, replace data with random characters or mock data, and delete data from your Salesforce org.

Satisfy Data Subject Access Requests

The Data Subject Access Request feature in Salesforce Customer 360 Privacy Center addresses your customers' right to obtain a copy of their personally identifiable information (PII) from your Salesforce org. Create a portability policy to identify customer PII found in various objects and fields. When customers request access to their personal data, securely send them a copy of their PII data using Portability API.

Provision Heroku Resources to Use Privacy Center

Salesforce Customer 360 Privacy Center uses Heroku for data processing and storage. The Privacy Center license includes add-on credits that you use to provision Heroku resources for the Data Retention feature.

To use the Data Retention feature in Customer 360 Privacy Center, allocate your Heroku credits to the following resources:

- Postgres Private 6
- Redis Private 7

Included with your purchase of Customer 360 Privacy Center are the following Heroku resources:

- Heroku Connect—10 million rows
- Heroku Private Space
- 2 Private Dynos

For more information about Heroku resources, visit Heroku Products.

Create Data Deletion, Retention, and Archiving Policies

Satisfy your customers' right to be forgotten requests and manage data retention in your org by creating policies that delete or make personally identifiable information (PII) anonymous at record or field levels. Use this feature to retain or archive data, replace data with random characters or mock data, and delete data from your Salesforce org.

<div style="float:right">

USER PERMISSIONS

To view and edit data:
- ModifyAllData or PrivacyDataAccess

</div>

To create data retention, deletion, and archiving policies, make sure that the Heroku add-on credits you received with your Privacy Center license are provisioned to the correct Heroku resources. For more information, see Provision Heroku Resources to Use Privacy Center.

1. From Setup, in the Quick Find box, enter `Privacy Center`. Select **Policies**, then click **New**.

2. Enter a name for your policy. The name must be alphanumeric, with no spaces or special characters. Click **Save & Edit**.

3. Under Run Frequency, indicate how often you want the policy to run. For right to be forgotten requests or to manually run the policy, set the frequency to **None**.

4. Under Objects & Fields, click the name of an object to run the policy on. Switch the object in the policy to Active.

5. Under Action On Data Copied to Heroku, choose to copy the original data, copy the edited data, or to not copy any data to Heroku.

6. Under Action on Data In Org, choose to edit or delete the data.

7. Select any child objects that you want to include in the policy, then click **Next**.

8. As an optional step, you can add data filters to child objects. A data filter captures fields you select on the child object that meet criteria you create. For example, apply a filter so that your policy only captures data created in the child object after a specific date.

9. Edit fields in the child object. If you don't select an action for the field, the field's data doesn't transfer to Heroku.

    a. To remove the field's data from your org, select **Delete**.

    b. To edit the field's data, select one of the following actions.

- Retain—Choose to copy existing data from your org to Heroku.
- Replace with Random Characters—Replace existing data with random alphanumeric characters.
- Replace from Library—Replace existing data with mock data from one of the provided libraries.

10. Click **Next**, then follow steps 7 and 8 for your parent object.

11. Click **Save**, then click **Activate**.

After your policy is activated, it runs at the frequency you set. To manually run the policy at any time, click **Run**.

Satisfy Data Subject Access Requests

The Data Subject Access Request feature in Salesforce Customer 360 Privacy Center addresses your customers' right to obtain a copy of their personally identifiable information (PII) from your Salesforce org. Create a portability policy to identify customer PII found in various objects and fields. When customers request access to their personal data, securely send them a copy of their PII data using Portability API.

Create a Portability Policy

The policy detects and displays any default and custom objects connected to the Account, Contact, Individual, Lead, Person, or User objects. You also individually select fields on an object that represent a customer's personally identifiable information (PII).

Monitor Data Subject Access Request Fulfillment with the Portability Log

Make sure that your Salesforce org fulfills every customer request to access personal data in accordance with data compliance law. Use the Portability Log in Customer 360 Privacy Center to see a history of all portability policies executed in your org.

Create a Portability Policy

The policy detects and displays any default and custom objects connected to the Account, Contact, Individual, Lead, Person, or User objects. You also individually select fields on an object that represent a customer's personally identifiable information (PII).

Starting with the Spring '21 release, Customer 360 Privacy Center automatically deletes files generated by Portability API after 60 days. You receive a reminder 7 days before a file is deleted.

1. From Setup, in the Quick Find box, enter `Privacy Center`. Select **Portability Policy**, then click **New**.

2. Under Policy Editor, click **Link New Object**. Choose related objects to add to the policy, then click **Save**.

3. In the Policy Editor, double-click an object name to see fields on the object.

4. Check the box next to any fields you want the policy to identify as PII. Click **Save**.

5. Enter a name for your policy. Activate the policy, then click **Save**.

6. On the Portability Policy page, find the name of your policy. Click the dropdown arrow, then click **Activate**.

After you activate the policy, run the Portability API to compile the identified PII. The Portability API returns a link to a secure file that your customer downloads to complete the request. For more information, see Portability.

Monitor Data Subject Access Request Fulfillment with the Portability Log

Make sure that your Salesforce org fulfills every customer request to access personal data in accordance with data compliance law. Use the Portability Log in Customer 360 Privacy Center to see a history of all portability policies executed in your org.

To use this feature in the Customer 360 Privacy Center, you need the Execute Data Subject Access Policies permission.

To view the Portability Log, from Setup, in the Quick Find box, enter `Customer 360 Privacy Center`. Select **Portability Log**. You can then customize the log to display information you want to see, such as when a policy finished executing or if your customer downloaded their portability file:

1. From the Portability Log dashboard, click the gear icon.

2. Click **Select Fields to Display**.

3. Choose the fields you want to see in the Portability Log. To add or remove selected fields from the log, use the arrows between the Available Fields box and the Visible Fields box. Optionally, to change the order that the fields appear in on the log, use the arrows next to the Visible Fields list.

4. Save your changes.

You can create charts and filters in addition to customizing the fields that appear in the log. You can't clone, delete, or share a Portability Log dashboard.

USE THE CONSENT EVENT STREAM

Use one stream to receive notifications about changes to consent fields or contact information on all core objects. When your users make a change to an object, an event is emitted into the stream with information about the change. This information is available to view for 24 hours.

The Consent Event Stream monitors changes to consent fields and contact information for these objects:

- Authorization Form Consent
- Contact
- Contact Point Consent
- Contact Point Email
- Contact Point Phone
- Contact Point Type Consent
- Communication Subscription Consent
- Individual
- Lead
- Party Consent
- Person Accounts
- User

1. From Setup, in the Quick Find Box, enter *Consent Event Stream*, then select **Consent Event Stream**.

2. Check the box next to **Use the consent event stream**.

3. Subscribe to the channel /event/ConsentEvent. For more information, see Subscribing to Platform Events

👁 **Example:** channel /event/ConsentEvent

```
{
  "data": {
    "schema": "GzuA-iAALq0ABxW_WNjlag",
    "payload": {
      "TenantId": null,
      "NewValues": "{\"ShouldForget\":true}",
      "ConsentCaptureSource":"com/salesforce/api/soap/47.0;client",
      "CreatedById": "0054J000002fRxBQAU",
      "ChangeType": 1,
      "ConsentCaptureType": null,
      "ChangeInitiator": "0054J000002HEa4QAG",
      "CreatedDate": "2019-11-18T01:36:39.536z",
      "RecordId": 0PK4J000000CabiWAC",
      "ChangeTimeStamp": "2019-11-18T01:36:37:000z",
      "GlobalPartyId": null,
      "ObjectName": "Individual"        }
    },
    "event": {
```

85

```
      "replayId": 287
    },
    "channel": "/event/ConsentEvent"
}
```

MANAGE DATA POLICIES FOR EINSTEIN FEATURES

We provide tools to help you honor customers' requests for how to handle their data. If you use Einstein Activity Capture, Inbox, Sales Cloud Einstein, or Service Cloud Einstein, you can control some aspects of how data is used. You can also delete email and event data.

Exclude People's Personal Data from Modeling and Predictions

If you use Sales Cloud Einstein, Service Cloud Einstein, or Einstein Call Coaching, it's easy to honor your customers' requests to exclude their personal data from factoring into machine learning models, and to stop generating predictions based on their personal data.

Exclude People's Personal Data from Modeling and Data Enrichment

If you use Einstein Activity Capture, Salesforce Inbox, or Einstein Automated Contacts, it's easy to honor your customers' requests to exclude their personal data from factoring into machine learning models. You also exclude personal data from being used by Salesforce features, such as Einstein Automated Contacts and Recommended Connections.

Delete Email and Events Logged by Einstein Activity Capture and Salesforce Inbox

Honor your customers' requests to delete their personal data in Salesforce email and events. It's easy to delete your customers' activities from storage outside of Salesforce and from the activity timeline. Engagement data is also deleted when the associated email is deleted.

Exclude People's Personal Data from Modeling and Predictions

If you use Sales Cloud Einstein, Service Cloud Einstein, or Einstein Call Coaching, it's easy to honor your customers' requests to exclude their personal data from factoring into machine learning models, and to stop generating predictions based on their personal data.

> 🛑 **Important:** If you use Salesforce Inbox, Einstein Activity Capture, or Einstein Automated Contacts, it's possible that you need to also exclude email data from machine learning models. Learn more in Exclude People's Personal Data from Modeling and Data Enrichment.

1. For any of the listed objects, create a custom field using the type Checkbox, and give it the API name *AI_HasOptedOutProfiling__c*.

   - Account
   - Activity
   - Case
   - Contact
   - Contact Role
   - Lead
   - Opportunity
   - Voice Call

2. For each record you want to exclude from modeling and future predictions, set the field value for that record to TRUE, or select the new checkbox in Salesforce.

Exclude People's Personal Data from Modeling and Data Enrichment

If you use Einstein Activity Capture, Salesforce Inbox, or Einstein Automated Contacts, it's easy to honor your customers' requests to exclude their personal data from factoring into machine learning models. You also exclude personal data from being used by Salesforce features, such as Einstein Automated Contacts and Recommended Connections.

> 🛑 **Important:** Keep in mind that these steps remove enriched data. But standard profile data still appears from Salesforce. For example, when you use Salesforce Inbox, profile data from Salesforce still appears.

1. From Setup, enter `Data Policies` in the Quick Find box, then select **Excluded from Machine Learning** under Data Policies.

2. Add the email addresses of the people to exclude

3. Click **Exclude** and confirm your selection.

4. We process the request after seven days and it can take up a month to complete. Check the status of your exclusions from the Excluded from Machine Learning page.

EDITIONS

Available in: Lightning Experience

Available with Sales Cloud in: **Essentials**, **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

Available with Sales Cloud Einstein, which is available for an extra cost in: **Enterprise**, **Performance**, and **Unlimited** Editions

Available with Inbox, which is available for an extra cost in: **Professional**, **Enterprise**, **Performance**, and **Unlimited** Editions

Available with High Velocity Sales, which is available for an extra cost in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To Exclude Data
- Customize Application OR Modify All Data

Delete Email and Events Logged by Einstein Activity Capture and Salesforce Inbox

Honor your customers' requests to delete their personal data in Salesforce email and events. It's easy to delete your customers' activities from storage outside of Salesforce and from the activity timeline. Engagement data is also deleted when the associated email is deleted.

> ⊘ **Important:** Keep in mind that these steps don't remove data stored in Salesforce or from your email services. Delete data from these locations manually.

1. From Setup, enter `Data Policies` in the Quick Find box, then select **Delete Email and Events** under Data Policies.

2. To delete activity by email address:
   a. On the By Email Address tab, add the email addresses of the people whose activity you want to delete.
   b. Choose whether to delete all past email and events or all one-to-one email messages and events that include the selected email addresses.
   c. Click **Delete**, and confirm your selection.

3. To delete activity by user:
   a. On the By User tab, add the email addresses or user names of the people whose activity you want to delete.
   b. Click **Delete**, and confirm your selection.
   c. To avoid data corruption when we stop capturing data for the user, deactivate the user in Salesforce. The user loses access to Inbox, but you can return access to Inbox and Einstein Activity Capture by provisioning the person as a new user.

4. We process the request after 7 days, and it can take up to a month to complete the request. Check the status of activity deletion on the Delete Email and Events page.

   > ⊘ **Important:**
   > - For Sales Cloud Einstein users, some delete jobs show a Completed status before all data is deleted. If you need details about what's been deleted, contact Salesforce Customer Support.
   > - If an email address or user with deleted activity doesn't appear in the deleted list, the data might already be removed, or Einstein Activity Capture doesn't log the user's activities.
   > - Scheduled emails are sent if the send date is within 60 days from the request to delete the user's activity.
   > - Regardless of the data retention period, non-identified data from activities is kept for up to two years and used with machine learning models and third-party data enrichment.

INDEX