Salesforce Privacy Center & Consent Management

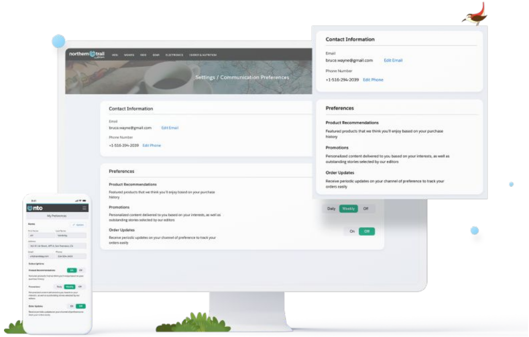
Svet Voloshin

What is it?

The Salesforce Privacy Center is a centralized platform provided by Salesforce for managing and protecting customer data privacy. It provides resources and tools to help organizations meet privacy requirements and regulations, such as the EU's General Data Protection Regulation (**GDPR**) and the California Consumer Privacy Act (**CCPA**).

The Salesforce Privacy Center includes features such as **data subject request management, data protection impact assessments, and privacy settings management**. It also provides access to resources such as guidance on privacy regulations, privacy training and education, and privacy-related product updates.

By using the Salesforce Privacy Center, organizations can proactively manage privacy risks and demonstrate their commitment to protecting customer data privacy.


northern trail
MEN WOMEN KIDS GEAR ELECTRONICS ENERGY & NUTRITION
Settings / Communication Preferences
nto
My Preferences

Contact Information

Email
bruce.wayne@gmail.com Edit Email

Phone Number
+1-516-294-2039 Edit Phone

Preferences

Product Recommendations
Featured products that we think you'll enjoy based on your purchase history

Promotions
Personalized content delivered to you based on your interests, as well as outstanding stories selected by our editors
Daily Weekly Off

Order Updates
Receive periodic updates on your channel of preference to track your orders easily
On Off

[Pricing: 15% of Net Spend](#)

What is GDPR?

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It came into effect on **May 25, 2018** and replaces the 1995 EU Data Protection Directive. The GDPR sets **strict rules for collecting, processing, and storing personal data** and gives individuals **more control over their personal information**. It applies to all organizations operating within the EU, as well as organizations outside of the EU if they offer goods or services to individuals in the EU.

The GDPR requires organizations to **obtain clear and affirmative consent from individuals** for the collection and processing of their personal data, to provide individuals with access to their personal data, and to securely store and protect that data. Organizations must also report data breaches to relevant authorities and affected individuals within 72 hours of becoming aware of the breach. The GDPR also gives individuals the right to have their personal data deleted, known as the “right to be forgotten.”

Penalties for non-compliance with the GDPR can be severe, including fines of up to 4% of a company’s annual global revenue or €20 million, whichever is greater.

What is CCPA?

The California Consumer Privacy Act (CCPA) is a privacy law in the state of California, USA that gives consumers the **right to control the use of their personal information by businesses**. The CCPA applies to **for-profit companies operating in California** that collect personal information from California residents, and the law grants consumers the right to know what personal information is being collected about them, the right to request that their information be deleted, and the right to opt-out of the sale of their personal information.

The CCPA also requires businesses to implement **reasonable security measures** to protect the personal information they collect, and to notify consumers in the event of a data breach that may result in the unauthorized exposure of their personal information. Additionally, the CCPA places restrictions on the collection and use of personal information of minors **under the age of 16**.

Overall, the CCPA is designed to give **California consumers** more control over their personal information and to increase transparency and accountability for businesses in the handling of personal information.

Right to be forgotten...

The "right to be forgotten" is a concept in data protection law that gives individuals the right to request the removal of personal information that is outdated, inaccurate, or no longer relevant. The right is often framed as a way to balance privacy rights with freedom of expression and the public's right to access information.

The right to be forgotten has been established as a legal principle in some European Union (EU) countries, including France and Spain. In 2014, the European Court of Justice ruled that **individuals have the right to ask search engines, such as Google, to remove links to personal information that is deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed."**

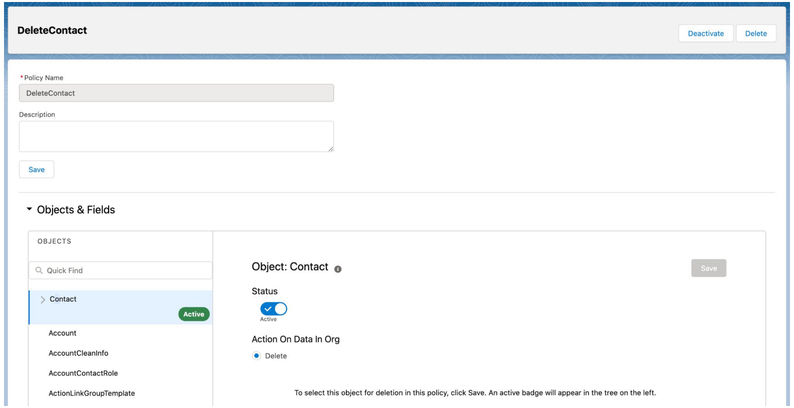
The right to be forgotten is still a **developing area of law**, and there is ongoing debate about how it should be applied and balanced against other rights and interests. In some cases, the right to be forgotten has been criticized for potentially stifling free speech and limiting access to information that is in the public interest.

Failure to manage risks - GDPR

- The GDPR is a comprehensive data protection law that regulates the collection, storage, and processing of personal data within the European Union (EU).
- Failure to manage privacy risks under the GDPR can result in significant administrative fines and penalties.
- The maximum fine under the GDPR is 4% of a company's annual global revenue or €20 million, whichever is greater.
- Failure to manage privacy risks under the GDPR can also result in legal action by individuals whose personal data has been affected.
- It can also lead to loss of customer trust and confidence, and damage to a company's reputation.
- To avoid these risks, businesses and organizations must implement strong data protection and privacy policies, invest in data security technologies and processes, and train their employees on data privacy and protection.

Right to be Forgotten Module

- Right to be Forgotten, through this module, is meant for **individual requests**.
- You can create a policy based off of an object, and then link any related objects to that, so for example, if a contact reaches out to you, you'd like to not only delete that contact's information, but any related case information, for example, that's a related object.
- Then, all you have to do when they reach out is enter in their Contact id, select the policy that you created that you'd like to run against it, and it will immediately queue up to be run in 24 hours.
- Or, if you select into it , you can have it run immediately. This is an SObject that you can also pull into any other reports.



DeleteContact

*Policy Name: DeleteContact

Description:

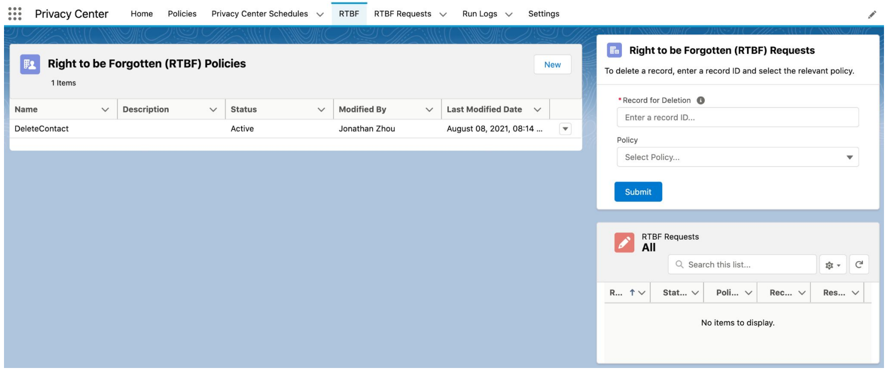
▾ Objects & Fields

Object: Contact

Status: Active

Action On Data In Org: ● Delete

To select this object for deletion in this policy, click Save. An active badge will appear in the tree on the left.



Right to be Forgotten (RTBF) Policies

1 Items

Name	Description	Status	Modified By	Last Modified Date
DeleteContact		Active	Jonathan Zhou	August 08, 2021, 08:14 ...

Right to be Forgotten (RTBF) Requests

To delete a record, enter a record ID and select the relevant policy.

*Record for Deletion: Enter a record ID...

Policy: Select Policy...

RTBF Requests
All

R...	Stat...	Poli...	Rec...	Res...

No items to display.

Data Residency Requirements

- Data residency requirements dictate where certain data must be stored and processed.
- These requirements are put in place to ensure the security and protection of sensitive or personal information.
- Data residency requirements can vary depending on the type of data and the jurisdiction in which it is collected.
- They can have significant implications for businesses and organizations that operate globally.
- They may require businesses to store and process data in multiple jurisdictions and comply with different data residency laws.
- Some countries have strict regulations around the export of certain types of data.
- The European Union's General Data Protection Regulation (GDPR) includes provisions on data residency.
- Other countries and regions, such as Australia and Canada, also have their own data residency requirements.

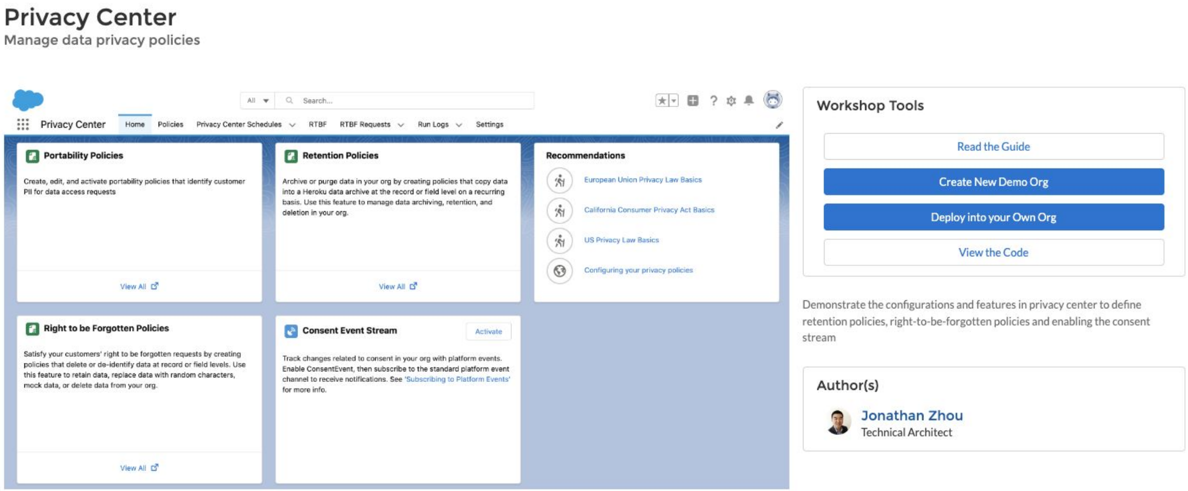
European Data Residency Laws

- **General Data Protection Regulation (GDPR)**: The GDPR is a comprehensive data protection law that regulates the collection, storage, and processing of personal data within the EU. The GDPR sets strict requirements for businesses and organizations in terms of data protection and privacy, and it imposes significant fines for non-compliance.
- **ePrivacy Regulation**: The ePrivacy Regulation is a proposed regulation that aims to harmonize and strengthen privacy rules for electronic communications in the EU. The regulation will cover areas such as cookies, spam, and confidentiality of communications, among others.
- **Electronic Communications Data Protection Regulation (eCDP)**: The eCDP is a regulation that sets out rules for the protection of personal data processed in the context of electronic communications services in the EU. The regulation covers areas such as data retention, location data, and the protection of communications content.
- **Network and Information Systems Directive (NIS Directive)**: The NIS Directive is a directive that sets out **cybersecurity requirements** for essential services, such as energy, transport, and healthcare, as well as digital service providers, such as cloud computing services. The directive requires these organizations to implement appropriate technical and organizational measures to ensure the security of network and information systems.

Privacy Center on Platform Demos

PlatformDemos.com

- This is a must!
- Quickly spin up a Scratch Org without DX
- Try out various products and features
- Significantly speed up your learning



Privacy Center

Manage data privacy policies

Portability Policies

Create, edit, and activate portability policies that identify customer PII for data access requests

View All

Retention Policies

Archive or purge data in your org by creating policies that copy data into a Heroku data archive at the record or field level on a recurring basis. Use this feature to manage data archiving, retention, and deletion in your org.

View All

Recommendations

- European Union Privacy Law Basics
- California Consumer Privacy Act Basics
- US Privacy Law Basics
- Configuring your privacy policies

Right to be Forgotten Policies

Satisfy your customers' right to be forgotten requests by creating policies that delete or de-identify data at record or field levels. Use this feature to retain data, replace data with random characters, mock data, or delete data from your org.

View All

Consent Event Stream

Activate

Track changes related to consent in your org with platform events. Enable ConsentEvent, then subscribe to the standard platform event channel to receive notifications. See 'Subscribing to Platform Events' for more info.

Workshop Tools

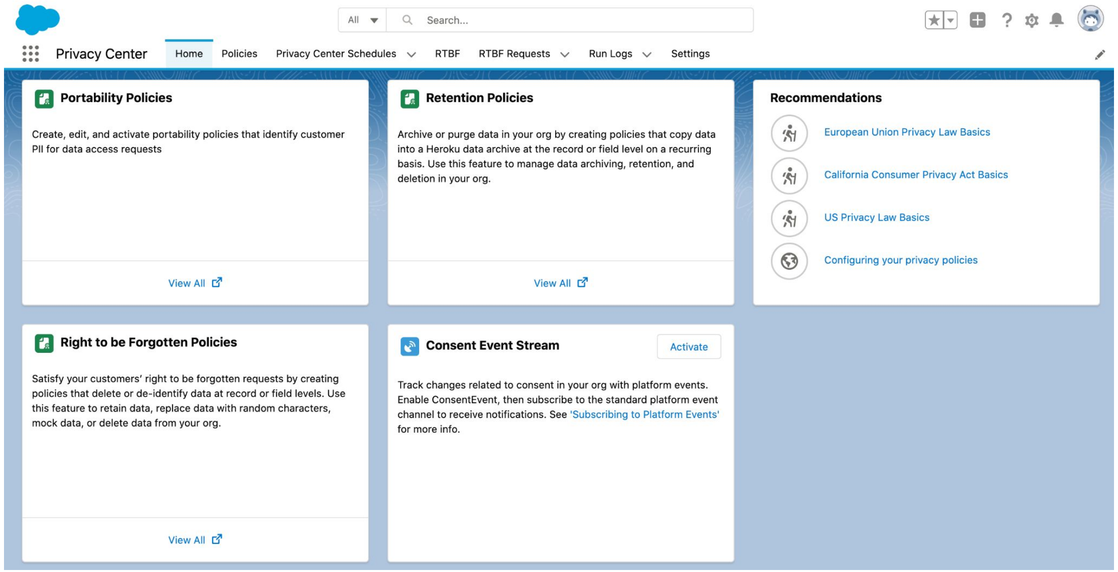
Demonstrate the configurations and features in privacy center to define retention policies, right-to-be-forgotten policies and enabling the consent stream

Author(s)

Jonathan Zhou
Technical Architect

Privacy Center Main Screen

You are now viewing the Privacy Center. Let's first look at how it can be applied to Right to be Forgotten and Data Retention requests.



Portability Policies

Create, edit, and activate portability policies that identify customer PII for data access requests

Retention Policies

Archive or purge data in your org by creating policies that copy data into a Heroku data archive at the record or field level on a recurring basis. Use this feature to manage data archiving, retention, and deletion in your org.

Recommendations

European Union Privacy Law Basics
California Consumer Privacy Act Basics
US Privacy Law Basics
Configuring your privacy policies

Right to be Forgotten Policies

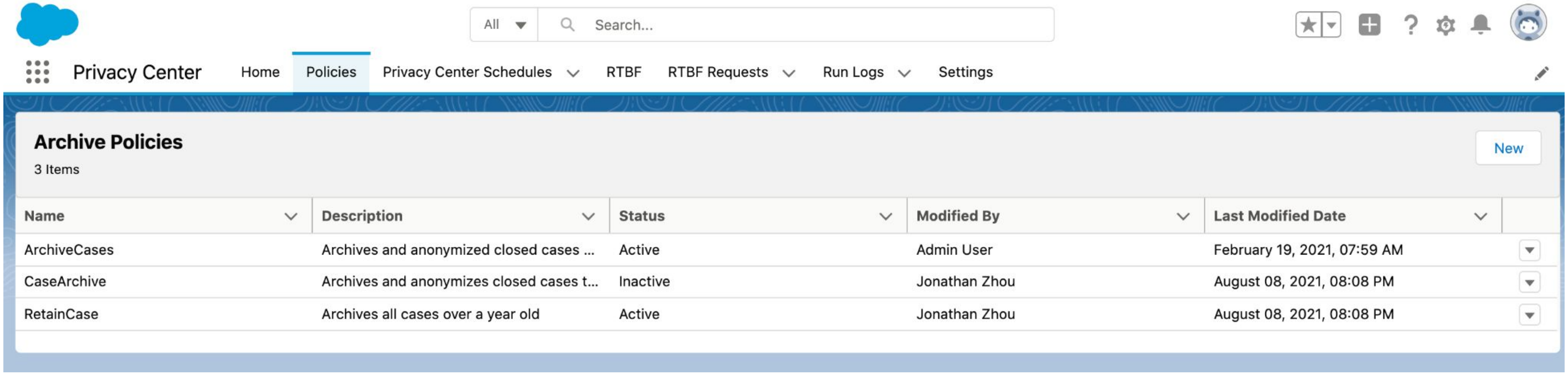
Satisfy your customers' right to be forgotten requests by creating policies that delete or de-identify data at record or field levels. Use this feature to retain data, replace data with random characters, mock data, or delete data from your org.

Consent Event Stream

Track changes related to consent in your org with platform events. Enable ConsentEvent, then subscribe to the standard platform event channel to receive notifications. See 'Subscribing to Platform Events' for more info.

Retention Policies

A few different circumstances were considered when creating Retention Policies. It is for subsets of data rather than a single record, and by developing automatic data erasure policies and business rules, right to be forgotten compliance is made simple.



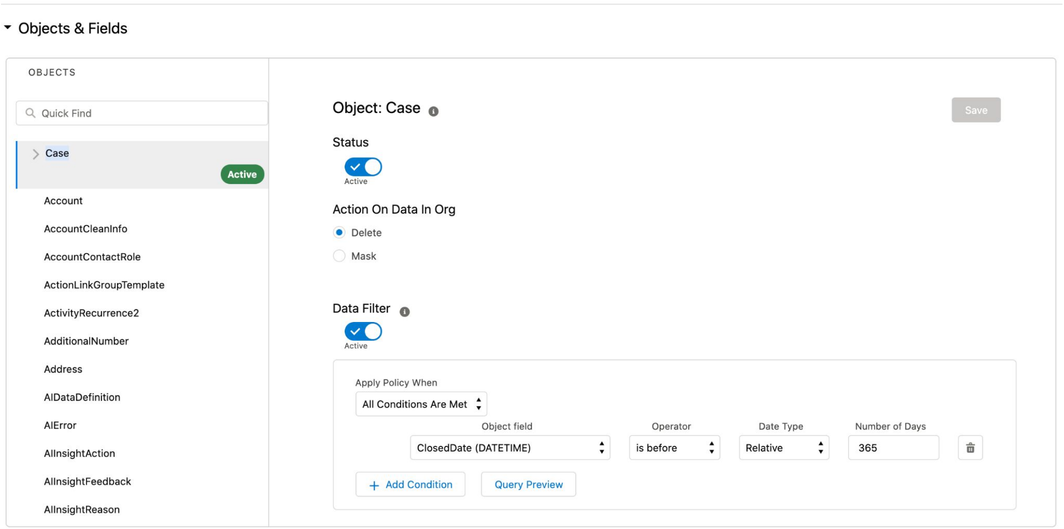
Archive Policies

3 Items

Name	Description	Status	Modified By	Last Modified Date
ArchiveCases	Archives and anonymized closed cases ...	Active	Admin User	February 19, 2021, 07:59 AM
CaseArchive	Archives and anonymizes closed cases t...	Inactive	Jonathan Zhou	August 08, 2021, 08:08 PM
RetainCase	Archives all cases over a year old	Active	Jonathan Zhou	August 08, 2021, 08:08 PM

Retention Policies

- Retention policies have the ability to mass-remove data from your Salesforce org and only **keep what is necessary**.
- You can **design rules to remove data** from your Salesforce org and place it in storage, for instance, if you get a right to be forgotten request but have a reason to keep it or if you didn't obtain consent for data that was in your org before GDPR.
- This enables you to adhere to the processing restriction principle as well. Consequently, what you should do is **make a policy off of the object Case** and activate it.



Object: Case

Status: Active

Action On Data In Org

● Delete

○ Mask

Data Filter: Active

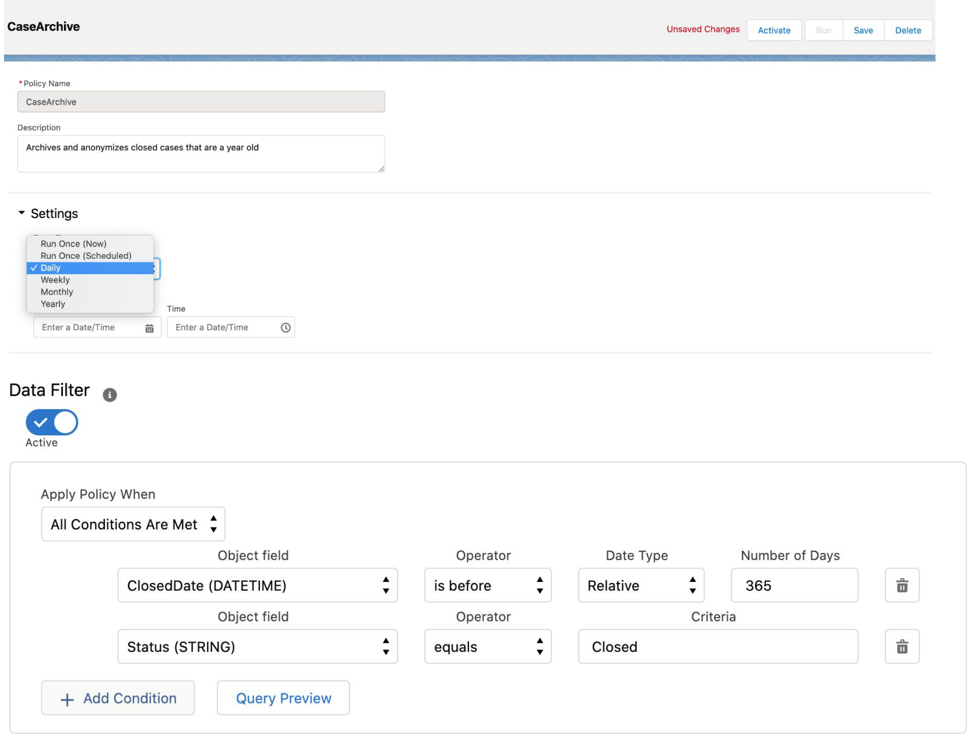
Apply Policy When: All Conditions Are Met

Object field	Operator	Date Type	Number of Days
ClosedDate (DATETIME)	is before	Relative	365

Scheduled Runs & Filtering

- You can also set it to run daily at the data and time that you specify, or weekly, monthly, or even yearly. Then you can choose the action that you would like to take.

- If you want to apply any filters, for example if certain fields in the condition is past a certain number of days,



CaseArchive

*Policy Name: CaseArchive

Description: Archives and anonymizes closed cases that are a year old

Settings

✓ Daily

Enter a Date/Time

Time: Enter a Date/Time

Data Filter

Active

Apply Policy When: All Conditions Are Met

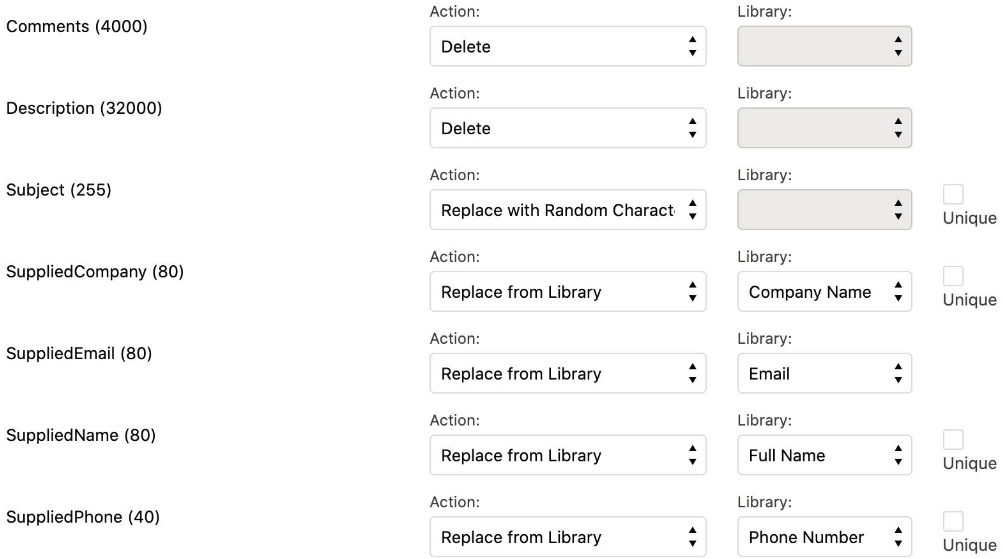
Object field	Operator	Date Type	Number of Days
ClosedDate (DATETIME)	is before	Relative	365

Object field	Operator	Criteria
Status (STRING)	equals	Closed

Additional benefits...

...and then you select which fields you'd like to retain, or the fields that you'd like to delete. Then you simply save, activate, and run your policy.

- Moving data out of production also helps **improve performance and reduce storage cost**.
- Data that is selected to be retained is archived into our **Heroku-backed storage** solution, to maintain access and scalability.
- Scheduling retention and archive policies also helps you with **easier management**, as we just showed.
- You can also use **external objects** to create a view of your retained data in your Salesforce org.



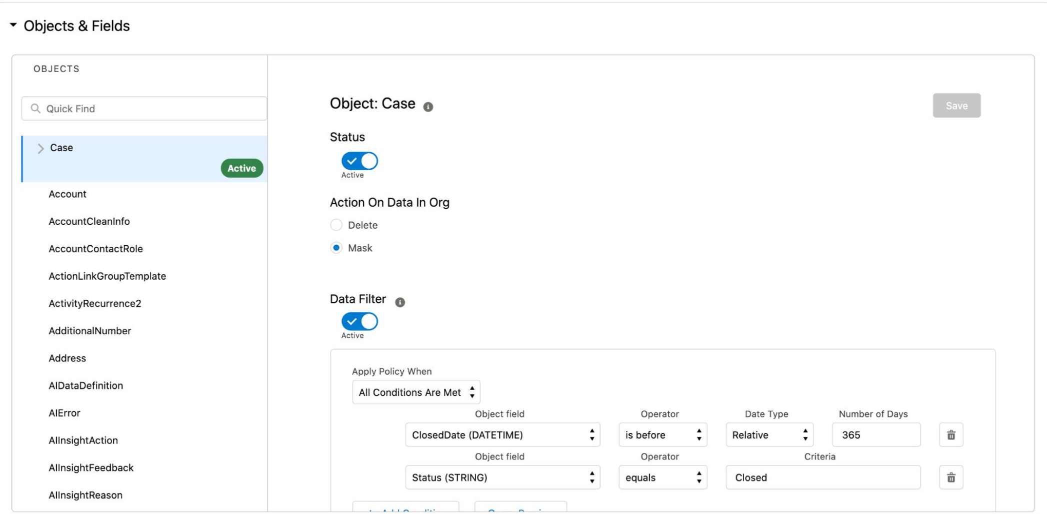
	Action:	Library:	
Comments (4000)	Delete		
Description (32000)	Delete		
Subject (255)	Replace with Random Charact		□ Unique
SuppliedCompany (80)	Replace from Library	Company Name	□ Unique
SuppliedEmail (80)	Replace from Library	Email	
SuppliedName (80)	Replace from Library	Full Name	□ Unique
SuppliedPhone (40)	Replace from Library	Phone Number	□ Unique

Data Masking

- Something else that you can do is mask data in your Salesforce org *en masse*.

- So similarly you can create the **same policies or filters**, and then you can choose whether to **delete**, **replace** with random characters, or replace from a library that we have pre-built for you.

- You can also choose to add in a unique identifier, and, if you have data classification on certain fields, a notification will pop up.



▾ Objects & Fields

OBJECTS

Quick Find

- Case — Active
- Account
- AccountCleanInfo
- AccountContactRole
- ActionLinkGroupTemplate
- ActivityRecurrence2
- AdditionalNumber
- Address
- AIDataDefinition
- AIError
- AIInsightAction
- AIInsightFeedback
- AIInsightReason

Object: Case

Save

Status: Active

Action On Data In Org

○ Delete

● Mask

Data Filter: Active

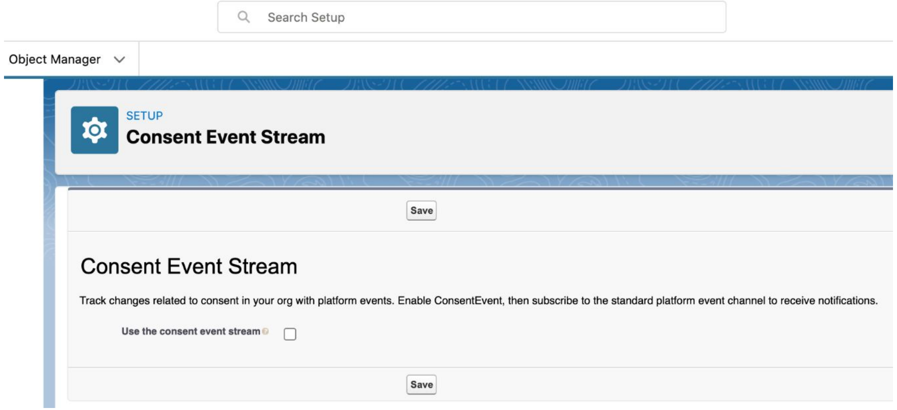
Apply Policy When: All Conditions Are Met

Object field	Operator	Date Type	Number of Days
ClosedDate (DATETIME)	is before	Relative	365

Object field	Operator	Criteria
Status (STRING)	equals	Closed

Consent Event Stream

- You also have access to Consent Event Stream.
- Consent Event Stream monitors changes to consent fields in contact information on Contacts, Individuals, Leads, Users, and other objects.
- When a change is made, a **platform event is published**.
- And that can be used to do things like **send event notifications, update other systems, or trigger a process to be run**.



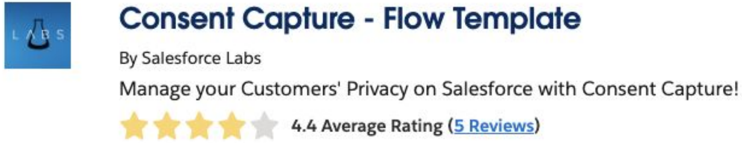
Consent Event Stream

Track changes related to consent in your org with platform events. Enable ConsentEvent, then subscribe to the standard platform event channel to receive notifications.

Use the consent event stream □

Salesforce Consent Capture

- Consent Capture gives you the tools you need to record customer preferences in line with your local privacy regulations.
- You can configure your own data use purposes and legal basis directly on the Salesforce platform, using standard objects.
- Using the consent records, you can manage the purpose, legal basis, and status of the consent that has been authorised by your contacts.
- These policies can be designed to fit your business process and become your ideal consent management process.

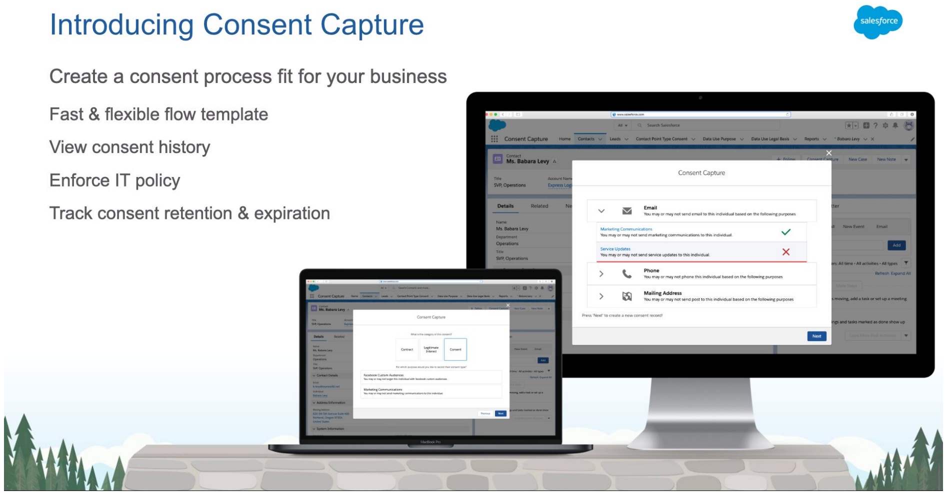


Consent Capture - Flow Template

By Salesforce Labs

Manage your Customers' Privacy on Salesforce with Consent Capture!

★★★★☆ 4.4 Average Rating (5 Reviews)



Introducing Consent Capture

Create a consent process fit for your business

Fast & flexible flow template

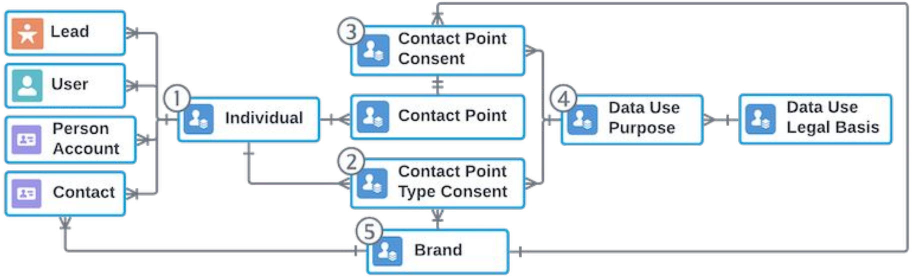
View consent history

Enforce IT policy

Track consent retention & expiration

Salesforce Consent Data Model

- The Salesforce Consent Data Model is the standard data model for managing consent at multiple levels, from global preferences to more granular controls.
- This data model, the **foundation** of Salesforce's long-term view of consent, considers the individual's entire experience, not just a single contact point.
- Any record that relates to an individual can have related consent considered within this model, including leads, users, person accounts, and contacts.
- It also provides flexibility to choose which level to manage consent initially.
- You can then add levels of granularity as business needs evolve or regulatory requirements change for managing that consent data.

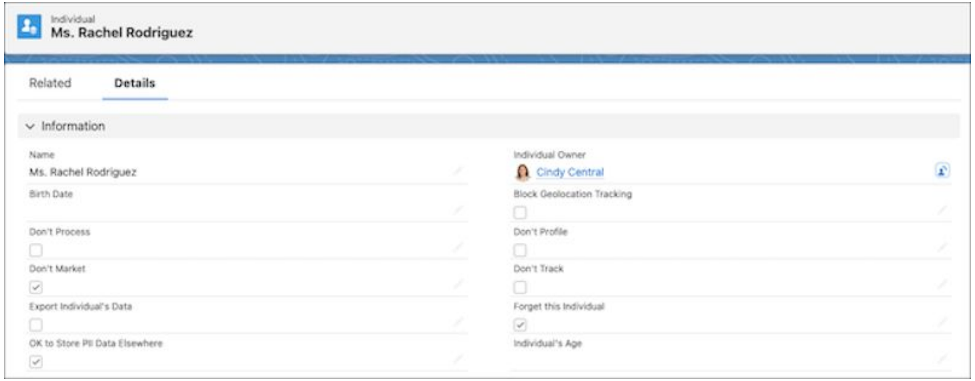


- Key Object: Individual
- Represents a customer's data privacy and protection preferences.
- Data privacy records based on the Individual object store your customers' preferences.
- Data privacy records are associated with related leads, contacts, person accounts, and users.

Global Consent

Global consent governs all-or-nothing consent settings managed on the **Individual object**. Global consent captures whether a customer approved communication.

Data privacy records based on the Individual object contain fields for managing global privacy settings.



Ms. Rachel Rodriguez

Name: Ms. Rachel Rodriguez

Individual Owner: Cindy Central

Birth Date:

Block Geolocation Tracking: □

Don't Process: □

Don't Profile: □

Don't Market: ☑

Don't Track: □

Export Individual's Data: □

Forget this Individual: ☑

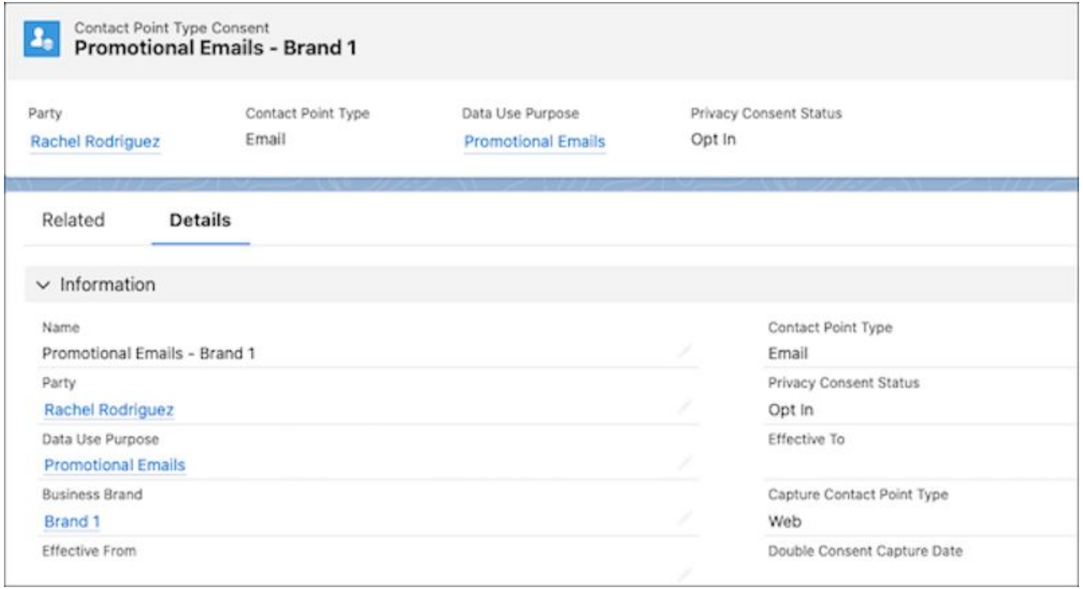
OK to Store PII Data Elsewhere: ☑

Individual's Age:

- Block Geolocation Tracking—Preference to not track geolocation on mobile devices,
- Don't Process—Preference to not process personal data, which can include collecting, storing, and sharing personal data.
- Don't Profile—Preference to not process data for predicting personal attributes, such as interests, behavior, and location.
- Don't Solicit—Preference to not solicit products and services,
- Don't Track—Preference to not track customer web activity and whether the customer opens email sent through Salesforce.
- Export Individual's Data—Preference to export personal data for delivery to the individual.
- Forget This Individual—Preference to delete records and personal data related to this individual.
- Individual's Age—Indication for whether the individual is considered to be a minor.
- OK to Store PII Data Elsewhere—Indication that you can store personally identifiable information outside of their legislation area. For example, you can store an EU citizen's personal data in the US.

Engagement Channel Consent

- Engagement channel consent is managed on the **ContactPointTypeConsent object**.
- Use **contact point type consent records** to enter consent preferences by a particular contact type, such as email or phone.



Contact Point Type Consent

Promotional Emails - Brand 1

Party	Contact Point Type	Data Use Purpose	Privacy Consent Status
Rachel Rodriguez	Email	Promotional Emails	Opt In

Name: Promotional Emails - Brand 1

Party: Rachel Rodriguez

Data Use Purpose: Promotional Emails

Business Brand: Brand 1

Effective From:

Contact Point Type: Email

Privacy Consent Status: Opt In

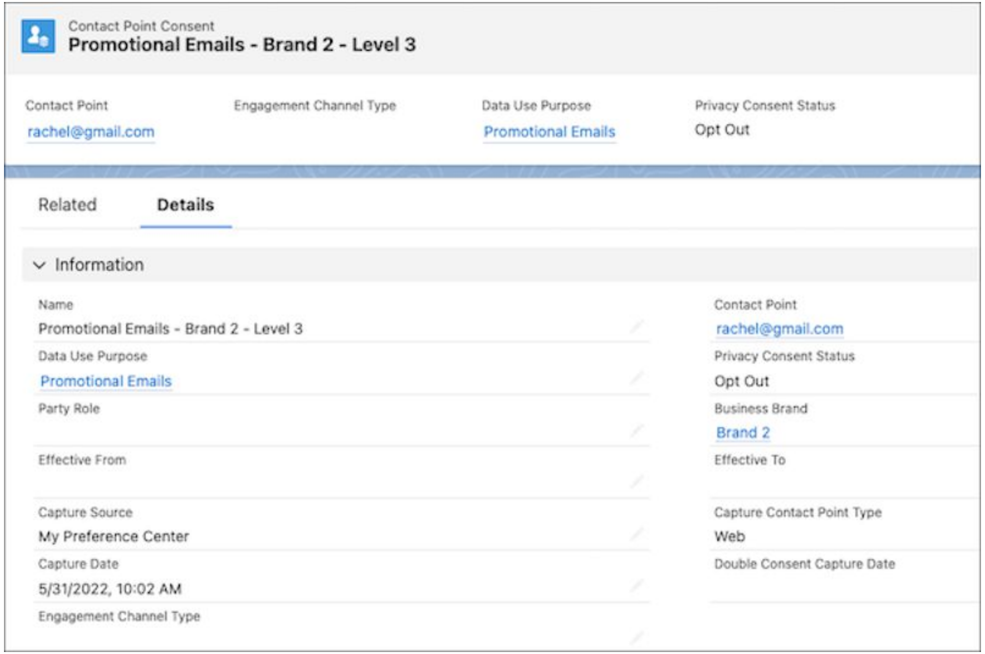
Effective To:

Capture Contact Point Type: Web

Double Consent Capture Date:

Contact Point Consent

- A customer's consent to be contacted is managed on the **ContactPoinConsent object**.
- **Contact point consent records** help you set consent by a specific contact point to be able to consider different consent preferences.
- For example, record a customer's preferences for using a personal email as opposed to a work email address.



Contact Point Consent
Promotional Emails - Brand 2 - Level 3

Contact Point: rachel@gmail.com
Engagement Channel Type:
Data Use Purpose: Promotional Emails
Privacy Consent Status: Opt Out

Name: Promotional Emails - Brand 2 - Level 3
Contact Point: rachel@gmail.com
Data Use Purpose: Promotional Emails
Privacy Consent Status: Opt Out
Party Role:
Business Brand: Brand 2
Effective From:
Effective To:
Capture Source: My Preference Center
Capture Contact Point Type: Web
Capture Date: 5/31/2022, 10:02 AM
Double Consent Capture Date:
Engagement Channel Type:

Data Use Purpose and Brand

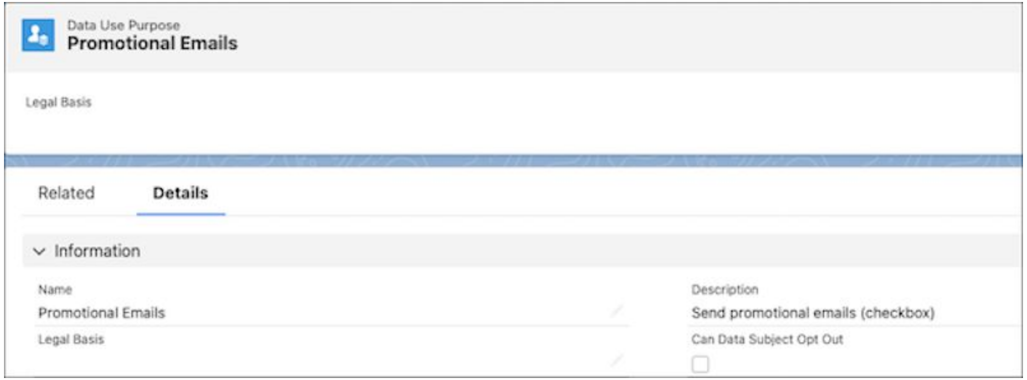
The DataUsePurpose object captures consent based on the reason for a communication. It’s displayed in data use purpose records. The reason can be any legitimate business interest, including items that:

- Are legal in nature, such as recall notices.
- Used for marketing purposes, such as weekly newsletters,
- Provide a service, such as warranty support.

Data use purpose can relate to Contact Point Type Consent and Contact Point Consent objects.

Brand

Brand is managed on the BusinessBrand object. While not strictly part of the consent data model, Brand helps you distinguish between privacy and consent preferences that vary between different brands operating in the same Salesforce org. The Brand object has a native relationship with Contact Point Type Consent and Contact Point Consent objects. To tie an originating contact record with its related contact point consent records in Marketing Cloud, we also connect Brand to the Contact object.



Data Use Purpose
Promotional Emails

Legal Basis

Name
Promotional Emails

Description
Send promotional emails (checkbox)

Legal Basis

Can Data Subject Opt Out
□

Consent Capture Levels

Consent Capture Levels refer to the different levels of consent that businesses can capture from their customers for various types of data processing and communication. Here are some common examples:

- **Implied consent:** Consent that is inferred based on the customer's actions or behavior, such as using a website or purchasing a product. This type of consent is generally considered to be less explicit and less reliable than other types of consent.
- **Explicit consent:** Consent that is given by the customer in a clear and unambiguous manner, such as by checking a box or signing a form. This type of consent is generally considered to be more reliable and legally defensible than implied consent.
- **Opt-in consent:** Consent that is given by the customer by actively choosing to opt-in to receive communication or to have their data processed. This type of consent is generally considered to be more robust and reliable than other types of consent, as it requires a positive action from the customer.
- **Opt-out consent:** Consent that is assumed unless the customer actively chooses to opt-out of receiving communication or having their data processed. This type of consent is generally considered to be less robust and less reliable than other types of consent, as it assumes that the customer is willing to receive communication or have their data processed unless they explicitly state otherwise.

Consent APIs

- Users sometimes store consent preferences inconsistently across different locations. To locate customer consent preferences across multiple records, use **Consent API** with specific Customer Data Platform parameters. Tracking consent preferences helps you and your users respect the most restrictive requests.

- Consent API aggregates consent settings across the Contact, Contact Point Type Consent, Data Use Purpose, Individual, Lead, Person Account, and User objects when the records have a lookup relationship. **The Consent API can’t locate records in which the email address field is protected by Shield Platform Encryption**.

- The Consent API **returns consent details based on a single action**, like email or track. The multi-action endpoint allows you to request multiple actions in a single API call.

Consent Capture Flow Template Overview

Consent Capture is a flow template that includes a set of tools and utilities to help you quickly implement a basic consent management system on Salesforce!

Using the new privacy & data governance objects in Salesforce, Consent Capture will help you:

1. Build your legal & marketing teams consent process into Salesforce
2. Give your users access to view an individual's active and expired consent records
3. Create new consent records
4. Create a customized flow that fits your business need

Consent Capture Flow Template Overview

The rest of the content is captured in the above Salesforce Presentation PDF

Resources

- YouTube: Managing Consent with Salesforce - CloudKettle
- Trailhead: Learn Privacy and Data Protection Law
- PlatformDemos.com: Privacy Center