DATA PROTECTION AND PRIVACY

Salesforce Privacy Center

Build and uphold customer trust by putting their data privacy first

© Copyright 2000–2021 salesforce.com, inc. All rights reserved. Salesforce is a registered trademark of salesforce.com, inc., as are other names and marks. Other marks appearing herein may be trademarks of their respective owners.
Contents

Introduction
Trust and Data Privacy
  Build Trust with Privacy Center
Privacy Center and Data Governance Laws
  Data Governance Across the World
What Privacy Center Can Do For You
  Manage Sensitive Data
  Streamline Preference Management
  Control Data Subject Access Requests
  Gain Insights and Track Changes
Consent Management Data Model
Resources
Introduction

In this data-driven world, customers are increasingly privacy-conscious. They want to buy from companies that prioritize privacy management and keep their personal information safe. For businesses, data protection and data management are key to building customer trust, remaining compliant with an evolving regulatory landscape, and increasing business value.

Data management is complex, but Privacy Center is up to the challenge. As a tool for your data management program, Privacy Center helps you maintain customer privacy through every stage of the data lifecycle. You can create policies that satisfy your customer’s right to be forgotten, meet data minimization requirements by removing inactive data from your Salesforce production org, or de-identify a customer’s personal data. You can even create portability policies that compile and deliver personal data quickly to customers in response to data subject access requests. With Privacy Center, prioritizing data privacy is just a click away.

Trust and Data Privacy

At Salesforce, we continuously monitor the global privacy landscape and adapt our privacy program to help protect customer data. By complying with regional privacy and data protection regulations worldwide, customers know they can count on us for managing even their most sensitive data.

BUILD TRUST WITH PRIVACY CENTER
Privacy Center helps your business handle data in the ways customers expect. Depending on where your customers live, you’re expected to comply with data requirements specific to their country, region, state, or industry. These requirements protect consumers’ rights to object to data collection, access the information collected, and request the deletion of their personal data.

For example, if your company collects customer requests about how personal data is stored, deleted, or transferred, your company can fulfill the requests using Privacy Center’s Retention Policies and Right to be Forgotten (RTBF) features. And throughout
that process, the Consent Event Stream helps you monitor any changes made to consent objects.

Privacy Center helps your company create policies that comply with your customers’ rights so that their data isn’t just protected, it’s also respected.

**Privacy Center and Data Governance Laws**

**DATA GOVERNANCE ACROSS THE WORLD**

Privacy Center was created to meet generalized requirements. But it’s also an adept solution for more specific regulations, which continue to evolve as data privacy takes on added significance globally.

For example, businesses that collect, store, or use personal information about European residents now must comply with the General Data Protection Regulation (GDPR). The GDPR regulates how companies can process personal data by focusing on seven major principles: fairness and transparency, purpose limitation, data minimization, accuracy, data deletion, security, and accountability. Privacy Center can directly assist with these specific GDPR principles:

- **Data Access**: An individual’s right to confirm with a data controller whether the organization is processing their personal data. And, if it is, the individual has the right to be informed about how that information is processed, why it’s being processed, and what other parties the information has been shared with.
- **Restriction of Processing**: An individual’s right to request that a controller stop accessing and modifying their personal data.
- **Data Portability**: An individual’s right to ask a controller to provide their personal data in a structured, commonly used, and machine-readable format. For example, the information can be transmitted to another company in a JSON file.
- **Right to Erasure, or the Right to be Forgotten**: An individual’s right to request that a data controller delete or remove their personal data in situations when the data is no longer needed for the original purpose and when the data subject withdraws consent. Another situation is when the data subject objects to the processing and the controller has no overriding legitimate interest in the processing.
While the European Union takes a comprehensive approach to data governance, the US takes a sectoral approach, with different industries, states, and data types governed by different privacy laws. The Consumer Financial Protection Bureau, Federal Reserve, and Office of the Comptroller of the Currency regulate the financial services industry, while the Department of Health and Human Services regulates the healthcare industry. Businesses in both industries must protect any personal data, and all businesses are required to effectively respond to security breaches of customer data.

An example of a state-specific regulation is the California Consumer Privacy Act (CCPA), which regulates the collection and usage of customer data similarly to the GDPR. Under the CCPA, Californian consumers have five primary rights, three of which Privacy Center can directly assist with.

- **Right to Access**: An individual’s right to request that a business disclose the categories and sources of personal information collected about them, the purpose for which the information was collected, and the third parties with which the business shares personal information.
- **Right to Opt Out**: An individual’s right at any time to tell businesses to stop selling their personal information.
- **Right to Request Deletion**: An individual’s right to request that businesses delete their personal information when such information was collected.

**What Privacy Center Can Do For You**

**UNIFIED DATA PRIVACY MANAGEMENT**

With Privacy Center, you can manage customer data through every step of the privacy lifecycle. Make the most of customer information by cataloging and categorizing collected data, assessing where it’s stored, and monitoring company access. Then pass that control onto customers by empowering them to set consent and privacy preferences, request a copy of their data, and see how their data’s processed.

At the same time, your company can orchestrate privacy events. Search and execute policy requests focused on deletion and portability, and connect cross-cloud by syncing with external systems and populating custom logs. Also, track data and consent by
documenting privacy activity. For example, you can view the lineage of personal data and consent to prove compliance with individual wishes. Or measure the effectiveness of your data collection by tracking metrics such as storage usage and time to close on data requests. You collect the data, and we help with everything else.

**Unified data privacy management**

**PRIVACY CENTER CAPABILITIES**

Privacy is multifaceted, and so is Privacy Center. Manage all your data needs in one place with each of Privacy Center’s capabilities.

<table>
<thead>
<tr>
<th>Privacy Center Capabilities</th>
<th>What It Does</th>
<th>Why It’s Important</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data privacy law compliance</strong></td>
<td>Manages the various components of data privacy laws and industry regulations.</td>
<td>Helps businesses comply with privacy laws like GDPR and fulfill customer requests about how their personal data is stored, deleted, and transferred.</td>
</tr>
<tr>
<td><strong>Data retention</strong></td>
<td>Creates policies to manage how long customer data is kept in Salesforce.</td>
<td>Helps businesses fulfill the customers’ Right to Be Forgotten and data retention requests by creating policies that delete or make data anonymous at record or field levels.</td>
</tr>
</tbody>
</table>
### Data subject rights

<table>
<thead>
<tr>
<th><strong>Data subject rights</strong></th>
<th>Automates how data is made anonymous or deleted from Salesforce, and compiles and securely transfers all personal data to customers.</th>
<th>Helps businesses automate customer requests to access, obtain, and transfer their personal data in Salesforce. Data subject rights automate these requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consent Event Stream</strong></td>
<td>Routes consent and contact information changes for all core objects to one location.</td>
<td>Helps businesses monitor changes to consent in one place so that businesses can easily fulfill new customer requests.</td>
</tr>
</tbody>
</table>

### Manage Sensitive Data

Privacy Center helps you simplify Right to be Forgotten and data retention requests. By creating policies and business rules for data erasures that run automatically, privacy compliance and RTBF is effortless.

**PRIVACY MANAGEMENT CAPABILITIES**

- **Simplify Privacy Compliance**
  Define business rules for data anonymization and data deletion, or retain data with legal basis and make it easier to adhere to privacy laws.

- **Execute Right to Be Forgotten Quickly**
  Create policies that capture the objects to delete, and run the policy on a specific record at any time, automating deletion.

- **Retain Only The Information You Need**
  Choose to mask or delete data from production, and select only the fields you want to keep for the retention store.

### DELETE & RETAIN DATA

You can meet Right to Be Forgotten requirements individually or en masse. Sometimes it makes sense to work on one record at a time. For example, if a data subject requests that you delete their data, you can remove only their individual data records. To do so,
create a policy in the **RTBF module** that aligns with your goals by choosing the best primary object:

- **Individual Object:** Designate Individual as your primary object to identify a wide range of personal data related to an individual. This related information includes any Account, Contact, or Leads records that you linked to the individual. Use Individual as the primary object when you want to remove everything about a customer from your org.

- **Contact or Personal Account Object:** Choose the Contact or Personal Account as your primary object when you want to remove everything about a customer from your org and you aren’t using the Individual object. The Contact and Personal Account objects give you access to data such as Cases, Contracts, Opportunities, and Quotes.

- **Lead Object:** Choose Lead as your primary object for times when you started marketing to a customer but haven’t yet converted them to an Account, Contact, or Opportunity. When Lead is your primary object, you can remove campaign records, feed comments containing personal data, and other data associated with the customer, such as SocialPost.

- **Case Object:** Select Case as your primary object when you want to remove data about an end customer who you interacted with only after they raised an issue. For example, use Case if you first interacted with a customer after they used Web to Case from a website. With Case as the primary object, you can remove any data that the customer provided as part of dealing with the case, such as Feed Comments.

After a request comes in, your admin simply enters the primary object’s record ID and chooses the appropriate policy to run. Then, based on admin preference, the policy runs immediately or in 24 hours.

Other times, you work at a larger scale. For example, you can have cases that are several years old that you’re keeping for historical, legal, or compliance reasons. Depending on your needs, you can use the **Retention Policy** module to increase privacy compliance:

- **Improve Data Protection:** Use retention to mask sensitive data that you have on cases and any associated records in your org. You can also keep a subset of the
original data off-platform for as long as legally required. With this feature, your
users can view the historical case count, but the data remains anonymized.

- **Practice Data Minimization:** Use retention to remove cases from your org, such as cases that have been closed for more than 2 years. You can then keep a subset of the original data in an off-platform store, allowing you to share that subset with users when required.

There are many reasons to practice data minimization or retention. For example, if you have a legal basis to retain information but not to process it, move the records and data that you’re required to retain into storage. There, they can be processed and viewed.

Or maybe your team tracks the invoices that you send out to specific customers. Your sales team can use a subset of this information as a historical account of your interactions with your customer, but other information isn’t useful.

In this case, you could define a retention policy that moves older records out of your org and into a retention store. Such a policy removes unnecessary data from your org while still making the information available to your sales team when required. And for instances when the data becomes outdated, you can completely remove it from your org and your retention store. For example, maybe your company holds invoices for only 7 years.

With Heroku-backed data storage, you can maintain access and scalability without cluttering up your org. But moving data into storage isn’t just about meeting data subject requests. When you move data out of production, you also improve performance and reduce storage cost.

**VIEWING RETAINED DATA**

Combined with the power of Salesforce Connect and Heroku Connect, Privacy Center helps you access the data chosen to be retained and stored outside of your org. Rather than copying data directly into your org, Salesforce Connect accesses external data on demand and in real time. With your data linked up, all that’s left for you to do is create a few external objects, and you’re able to view your retained data right in your org.
Streamline Preference Management

With the help of the Preference Center app, included as part of Privacy Center, customers can choose when, how, and why you contact them.

PREFERENCE MANAGEMENT CAPABILITIES

- **Low Code Preference Form UX**
  Create preference forms to capture consent and preferences with a clicks and config approach.

- **Use Anywhere and Customize**
  Generate code at the click of a button to drop into any website and customize to your company’s branding.

- **Design Self-Service Experiences**
  Use Experience Cloud and add the form to a Customer Account Portal to allow users to update their preferences.

LET PREFERENCE BUILDER CUSTOMIZE CUSTOMER RELATIONSHIPS

Use Preference Builder to create fully customizable forms that ask customers to specify exactly how you can use their data. What products or offers do they want to be contacted about? How often do they want to be contacted? What channels can you use to contact them? You can even add the option of unsubscribing from all communications.

After you create a form, embed it on a web page and provide access as a link at the bottom of any emails that you send to customers. Then they simply click the link, and they’re directed to the form you made, where they can indicate their communication preferences. Their responses are then fed into your core Salesforce data, meaning you always have the latest updates. And with a focus on low code, Preference Center makes it simple to match the preference form to your branding.

HOW SHOULD I USE PREFERENCE CENTER?

Preference Center assists you in centralizing consent, particularly when you have a multi-cloud configuration. This diagram shows that many customers use a mix of standard or custom consent objects that are synced to external clouds, such as Marketing Cloud or Pardot.
While the approaches are varied, the objectives are generally the same: to track whether you can email or contact a person on a channel for a particular data use purpose. For example, “Can I send an email to Astro at astro@salesforce.com for Product Updates?”

To capture the data for this requirement, the end customer needs a way to express their consent to receive communications. External clouds provide capabilities to capture customer preferences through their own Preference Builder tools, but they don’t capture a complete picture of the customer’s consent. They also often require customizations to send data changes back to the central Salesforce org.

In the new model, for products such as Marketing Cloud or Pardot, you can replace your tool-specific preference centers with a centralized preference form that runs in your core Salesforce org.

This approach reduces the effort required to build and capture a single source of customer consent, and it allows support for more complex consent options. It also allows you to capture additional compliance data, such as the consent captured date,
time, and source. This information is particularly important for demonstrating customer consent during auditing.

So when Astro opts in for Product Updates, you can store this data, along with information such as the duration the consent is valid for, and details about the channel. You also instantly have that information available inside the Salesforce org, which can be synced back to other clouds.

**EASY ACCESS FOR YOU AND YOUR USER**

Publish, edit, or delete your configurations in one location with your Preference Center dashboard. You can even create multiple versions of your configurations to make sure that you always ask the right questions to the right customers. The dashboard also provides you with a bird’s-eye view of your preference management, showing you which configurations are published, when they were last edited, who modified them, and more.

If you use Experience Cloud, you’re also able to set up a self-service option. Add your preference form to a Customer Account Portal, and users can update their own preferences at any time just by logging in.

**Control Data Subject Access Requests**

Privacy Center helps you create and monitor data policies quickly in response to data subject access requests (DSARs). By managing customer requests for personal data, you give them access to and control over their data.

**DATA SUBJECT ACCESS REQUESTS CAPABILITIES**

- **Identify and Compile Customer Personal Data**
  Define policies to allow customers to access, obtain, and transfer their personal data in your org.
- **Share Personal Data with Customers**
  Generate personal data files quickly and share the data with your customers securely.
- **Monitor All DSARs**
Check the progress of DSARs, and see a history of past and ongoing requests from customers.

**FULFILL CUSTOMER REQUESTS FOR PERSONAL DATA**
In line with their right to portability, you can create policies that identify and compile customer personal data. Whether a customer wants to know what data you collected or asks for a copy of that information to be sent to them, Privacy Center helps you create personal data files that can be shared securely with data subjects. You can also track the progress of current DSARs and access past requests to ensure that they were fulfilled.

**Gain Insights and Track Changes**
Privacy Center makes measuring the efficacy of your privacy program a breeze. With Privacy Analytics and Consent Event Stream, you have the tools to see the big picture of your privacy program.

**DATA TRACKING & VISUALIZATION CAPABILITIES**

- **Learn More About Data Subject Requests**
  Use Privacy Analytics to see which channels customers are using to grant consent and the data use purposes they give consent to.

- **Visualize Data Subject Requests**
  See how many requests your team is receiving and their status, and track whether data subjects responded to a consent request.

- **Track Consent Data**
  Receive notifications about changes to consent or contact information on all core objects in a single stream.

**KEEP TABS ON YOUR PRIVACY PROGRAM**
Privacy Analytics helps you keep data compliance and privacy at the center of your business. For a better idea of your customer’s consent model, monitor the contact channels that customers use to grant consent and what they’re providing consent for. Or track the status and number of data subjects you receive. You can also track how your team responds to the requests.
With Consent Event Stream, you’re able to follow consent data and sync privacy events externally. When consent or contact information is changed, you receive a notification in a single stream. And because you can distribute consent and privacy events to external systems, you can ensure that you’re always on the same page.

**Consent Management Data Model**

The power of Privacy Center is rooted in its consent management data model, which organizes and defines how each data element relates to the others. Built with different levels of consent, our data model gives precise control to you and your customers.

**DATA PRIVACY OBJECTS**

The consent management data model uses five levels of consent, all of which focus on varying degrees of granularity. Together, they help you and your customer define how and why you can contact customers, and what data your business can use, collect, share, or sell.

**Level 0 - Individual Consent**

In this level, consent objects relate directly to the Contact, Lead, and User records via the Individual object. These objects establish the foundation for the data model.

**Level 1 - Party Consent**
The Party Consent level is a slight modification on Individual Consent, in that it enables you to store data on how you obtained certain information or what type of consent was given. This level provides information on consent against a particular person or group, which we call a party.

For example, this level individually defines whether data can be shared, sold, collected, or profiled. It also allows you to flag data subject rights such as the right to portability or the right to be forgotten. For example, one customer requests that you don’t share or sell their data but is fine with you collecting their data, while another customer requests that you don’t share, sell, or collect their information.

The Individual object can also unify different roles. For example, a Contact, a User, a Person Account, and a Lead can all represent the same person. To tie each of these objects to a single individual and consolidate duplicate records without merging data, use the Individual object.

Level 2 - Channel Consent
At the Channel Consent level, the consent permissions become more specific and focus on the channels you’re allowed to use to contact your customers. This consent is represented through the Contact Point Type Consent (CPTC) object, which is tied to the Individual object. In this structure, each record represents consent to receive communication at the channel level, for example, through email, phone, fax, or SMS. Using the engagement channel entity, you can represent any channel you want. For example, a customer specifies that you can email them to collect information but not call them.

The CPTC object also includes information about when the consent is effective, how long the consent is valid, how the consent was captured, and what the Data Use Purpose is for the consent.

Level 3 - Contact Point
The Contact Point level is even more granular than the Channel Consent level because it specifies the contact points you can use in a given channel for a customer. Contact Point objects include the Contact Point Email, Phone, and Address objects, which allow you to store any number of email addresses, phone numbers, and physical addresses
for your users. These contact points are tied to the Individual, Accounts, or Person Accounts objects.

Contact Point Consent then grants consent against these objects so that you can grant consent to a specific phone number, email address, or physical address for a specific channel. For example, a customer can give permission for you to email them through their work email address but not through their personal email address.

**Level 4 - Data Use**
The final level of the data model focuses on data use, so it's related to the Contact Point and Channel Consent objects. With Data Use Purpose, a customer specifies the reasons that you can contact them through their preferred means. The Data Use Purpose object links to Contact Point Type Consent and Contact Point Consent, which allows you to add a purpose at the channel or point consent level. For example, a customer gives you permission to email them through their work email address, but only for the Data Use Purpose of new product updates.

Level 4 consent can also be captured through the subscription objects, which allow your user to subscribe to recurring communication on a particular channel for a particular contact point. For example, a user receives weekly information via SMS on their work phone and receives a monthly newsletter via email to their personal email address.

**Subscription Consent**
Related to the Contact Point object, Subscription Consent allows customers to specify consent for any recurring communication. Subscription Consent has two child objects: Subscription Timing and Subscription-Channel. With Subscription Timing, customers can specify the timing of any recurrent communication. For example, “Send me this weekly.” With Subscription-Channel, customers can specify what they receive communication on and through what channel they receive it. For example, “Send me product updates via SMS.”

**AUTHORIZATION FORMS**
Privacy Center uses authorization forms to track privacy policy and form management. They house information and consent pertaining to signed or agreed-to documents,
such as terms and conditions, privacy policies, and program signups. Each authorization form has associated objects that support use cases and relate to consent, text, and purpose.

**Authorization Form**
The Authorization Form object represents the specific name, version, and effective dates of a form that is associated with consent. With this object, you can determine if the document is the latest version of a named form. You can also link a form to its default text version, which presents the specific text to display if no other indication is provided. For example, the form can be a privacy policy or a list of terms and conditions that you ask your users to agree to.

**Authorization Form Text**
The Authorization Form Text object represents an authorization form’s text and language settings and houses information about the different versions of the text that are related to the privacy policy. This object is commonly used to distinguish between versions of the same form that differ in language, regional dialect, or local specifics. For example, you can use it to support differences in jurisdiction, contact data, or the metadata surrounding information collection.

**Authorization Form Consent**
The Authorization Form Consent object represents the date and way in which a user consented to an authorization form. It helps track the consent that the specific user has granted as it relates to the privacy policy. For example, this object can collect data on who has consent, when they consented, how they consented, and to which version of the form they consented to. When connected to one or more data use purposes, the Authorization Form can also indicate the use cases covered in the form along with their corresponding legal basis.

**CONSENT APIs**
Privacy Center enables you to update your consent permissions with Consent Read API and Consent Write API.

**Consent Read API**
With Consent Read API, you can interface with consent data, which can be useful for checking if you have permission to perform an action. For example, you can check
whether you’re allowed to email a user. The API then checks whether the user has opted out of email communication for a specific contact point and returns the answer to you.

Consent Write API
With Consent Write API, you can write consent stored in multiple locations, which can be useful if you want to update the appropriate consent objects in a single action. For example, you can opt out a user’s email from emails. The API then updates the relevant objects, in this case Contact Email Opt-Out, Contact Point, and Contact Point Consent.

Resources
For a more comprehensive overview of privacy and data governance, take the Learn Privacy and Data Protection Law trail. Although Privacy Center supports your business in privacy compliance, your legal team can help you identify the specific laws relevant to your business.

- Learn Privacy and Data Protection Law
- European Union Privacy Law Basics
- California Consumer Privacy Act Basics
- US Privacy Law Basics
- Privacy Center Definitions
- Salesforce Privacy Center Implementation Guide
- Salesforce Platform: Privacy Center