

Best Practices for Data Privacy on Salesforce



Privacy law is constantly evolving and compliance with data privacy regulations can seem complex. Privacy is a fundamental right, and recent regulations are a reflection of the increasing expectation of individuals to have control over the use of their personal data. There is an opportunity to earn customer trust and loyalty for those companies who are able to exceed their customers' expectations for transparently managing their personal data.

Salesforce enables you to exceed customer expectations by putting them, and their data, in the center of everything you do. Here are some things to consider as you build your business processes on Salesforce with an eye toward your data privacy regulation obligations and market sentiments.

This document does not provide legal advice and the information we present may not take into account future changes in laws and regulations. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

Build Your Knowledge

- **Carefully review all of the content at, and linked from, the [Salesforce Data Privacy Overview page](#).** This is a nearly comprehensive jumping-off point to a broad spectrum of resources to assist you on your data privacy journey with Salesforce.
- The importance of a sound governance program cannot be overstated. From within the [Trailblazer Community](#), search for “Governance” to discover whitepapers and Accelerators.
- Search [Trailhead](#), Salesforce’s free, on-line learning portal, for “data privacy” for guided learning on the topic.

Standard Features

Salesforce provides numerous building blocks out-of-the-box (no additional cost) to support your implementation of your privacy processes.

- One of the first steps of most any security or compliance initiative is a data classification exercise. Salesforce now provides metadata fields on every standard and custom field to support the [classification of data on-platform](#) where that knowledge can be actionable via flows and security policies - simple yet powerful!

- A [robust schema](#) is provided for you to store data subject preferences and requests, plus document how you've complied with data privacy regulations. No need to build it from scratch, and it just might help identify use cases you've not yet recognized.
- To assist with gathering consent, Salesforce Labs offers a free [Consent Capture Flow Template](#) and [Community Cookie Consent](#) component on AppExchange.
- The [Consent API](#) helps you honor data subject preferences. Leverage it to do some of the dicey, dirty work of assessing consent for you.
- The newest addition, [Consent Event Stream](#), provides the means of informing other systems and processes of changes to consent fields or contact information on core objects.
- The [Data Privacy and Protection](#) help article and its child articles provide considerations for honoring data subject requests by identifying the standard objects/fields that commonly contain PII. You'll still want to review everything else in light of your unique usage though. No one should consider this to be a comprehensive list of PII in any given org.
- Data privacy regulations commonly require that the confidentiality and integrity of sensitive data be protected via mature data information security practices. Ensure that your organization reviews the [Salesforce Security Guide](#) which details configurable security features. The Salesforce platform includes a free security [Health Check](#) tool that checks your security configuration against a recommended baseline, provides an overall score, and recommends changes to consider.
- Emerging data privacy regulation includes requirements for accessibility (compatibility with screen readers, etc.). Besides, 20% of the population (your market and employment pool) reports some form of disability.
 - Salesforce is committed to providing on-demand enterprise applications accessible to all individuals. To help meet our goal of [universal design](#), Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA to the extent possible.
 - The Salesforce mobile app provides users working with screen readers and other accessibility features a [fully accessible mobile experience](#).
 - If you want to learn more about accessible Salesforce design, testing, and development best practices, take our [Get Started with Web Accessibility Trail](#).
- Consistently execute your compliance-related business processes via the [platform's automation capabilities](#).

Advanced Features

If your organization is looking for something a little more turnkey or needs to decrease security and compliance risk, Salesforce is hard at work growing your options.

- [Privacy Center](#) is a new add-on product so you can expect rapid evolution, but initial features include:
 - Data Retention and Archive - Manage data lifecycle and adhere to regulations with data retention policies and data archival
 - Data Subject Rights - Automate data subject rights management with deletion, anonymization, and data access policies
 - Privacy Analytics - Data Privacy Analytics to help keep data compliance and privacy at the center of the business
- Monitor and conditionally manage data access with the [Event Monitoring](#) add-on feature. Its forensic-level logging identifies who accessed what and when. Its Transaction Security feature can enforce custom policies such as preventing the export of any report that contains any field that has been classified as confidential. If you have not looked at Event Monitoring recently, you might be blown away by how it has continued to blossom!
- Do developers and/or test users have access to sensitive data in your sandboxes? Eliminate PII from your sandboxes after refreshing from production with our new [Data Mask](#) add-on. This tool allows you to obfuscate or delete the data in whichever fields you specify, thereby fully supporting development and testing efforts while adhering to your organization's least privilege data access model. Obfuscating contact details in lower environments could also avoid accidental communications to data subjects resulting from development and testing activities.

Additional Considerations

- [What Is CCPA? The California Consumer Privacy Act Checklist](#)
- The [Salesforce Best Practices Around IT SOX Compliance](#) guide contains information that is also applicable to data privacy regulations.
- Consider consolidating other systems/repositories into your Salesforce org to reduce your governance efforts and bring consistency to your data privacy practices.

Salesforce recognizes that data privacy regulations are continually evolving and is actively working to grow our product offerings in this area. If you would like additional information about how Salesforce supports customers in specific regions or industries, visit our privacy website: **salesforce.com/privacy**.
