Give your customers more choice than a simple, "do business with us, 'yes' or 'no'." While the privacy law landscape is constantly evolving, and compliance with data privacy regulations can seem complex, they also are an opportunity to exceed customer expectations by putting them, and their data, in the center of everything you do.

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 that are able to exceed their customers’ expectations for transparently managing their personal data.

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.

- **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.

- Watch the video [Getting Started with EU Privacy (GDPR)](https://example.com). It presents an excellent overview that is relevant to data privacy regulations in general, regardless of where you operate.

- 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](https://example.com) where that knowledge can be actionable via flows and security policies.

- **Store and honor data subject preferences** with standard features that provide building blocks to address data privacy regulations. Consent can be managed to significant granularity - by endpoint and purpose. For example, “John can be called only on his work number for account and billing purposes, may be texted on his mobile for the same purposes, may be marketed only via his work email, and may not be contacted via fax, personal email, or personal phone.”
○ The Consent API provides the tools to aggregate consent information stored across multiple objects to ensure that when you make contact with a customer you are respecting the privacy preferences they have selected.

○ To assist with gathering consent, Salesforce Labs offers a free Consent Capture Flow Template on AppExchange.

- The Data Privacy and Protection help article and its child articles provide considerations for honoring data subject requests. In short, searching, filtering, reporting, exporting, and deleting are bread-and-butter functions within the Salesforce platform. Flows/automation enable your users to apply these basic functions in a planned and consistent means to meet data subject requests in the context of your unique business model.

- 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 all 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.

- Monitor and conditionally manage data access with the Event Monitoring (EM) add-on feature. Event Monitoring’s Transaction Security feature can be used to enforce policies such as preventing the export of any report that contains any field that has been classified as confidential. Additionally, it can help with verification of unauthorized access and identifying who accessed what and when. Here is a great session from Dreamforce 2019 around How to Enhance Your Privacy Program with Salesforce’s Data Privacy Program (starting at the 17:24 mark, but the entire video is great!).

- The Salesforce Best Practices Around IT SOX Compliance guide contains information that is also applicable to data privacy regulations.

- 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 QA efforts while adhering to your organization’s least privilege data access model. Data Mask is 100% native to the Salesforce platform, avoiding the need to vet the security and compliance of a separate platform. Obfuscating contact details in lower environments could also avoid accidental communications to data subjects resulting from development and testing activities.

- We recommend reviewing the numerous Certifications, Standards and Regulations with which Salesforce complies - such as C5 (ISAE 3000) and Privacy Shield - as verified by relevant third party assessments.

- Accessibility is an important topic. Companies should be mindful of accessibility for their users, and below are a few points to consider:

  ○ 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.

- There are additional features to be considered when reviewing your organization’s compliance with the CCPA: classification of data, Community Cloud, Field Audit Trail, Field Audit Trail, and the platform’s automation capabilities.

- Salesforce has over 5,000 technology solutions available on the AppExchange, and there are many offerings that address privacy, consent, GDPR, and CCPA.

- Consider consolidating other systems/repositories into your Salesforce org to reduce your governance efforts and bring consistency to your data privacy practices.

This paper focuses on the GDPR and CCPA, however Salesforce recognizes that they are only two points on a continually evolving regulatory journey. If you would like additional information about how Salesforce supports customers in other regions or industries, visit our privacy website: salesforce.com/privacy.