Key Privacy Considerations Checklist

At Salesforce, Trust is our number one value. As part of that commitment to trust, we want to enable our customers with the tools they need to make decisions about their own privacy compliance. Compliance is always a shared partnership between Salesforce and its customers, meaning that Salesforce commits to complying with its own obligations, but also to supporting its customers on their compliance journeys. As part of this commitment, Salesforce has not only developed products that will help customers to meet their own compliance goals, but it also has created a number of dedicated resources like the checklist below where our customers can think through some of their own obligations.

For more resources, please see Salesforce's dedicated privacy website which includes FAQs on local and industry specific privacy laws. We also recommend you review our Privacy and Ethical Use Principles Guiding our Response to COVID-19, and we have incorporated the principles that guided our Work.com product response into the checklist below.

When purchasing or implementing any new product or service, the checklist below may serve as a first step for members of the legal or compliance teams when thinking through any privacy obligations. If you have any questions about the requirements included in this checklist, please speak to your legal counsel to see how they apply to your specific situation.

✔	
Privacy and Ethical Use Principles	
☐	**Protect human rights and equality.** Solutions should not adversely affect already vulnerable populations. **Action**: Ensure your organization has considered ensuring it does not exclude users — especially those who are already vulnerable — or deny essential services.
☐	**Transparency.** Trust starts with transparency. Solutions should give individuals timely, accessible, and easily understandable notice of how their data is being collected and used, how their data is protected, and their rights to control the use of that data. **Action**: This may be achieved through a comprehensive and up to date **privacy notice** covering the collection (or "processing") carried out by your organization as part of the product or service. Make the notice easily accessible to all individuals who will either use the product or service or whose data will be collected as part of it.
☐	**Minimize data collection.** Collect and retain only the data that is essential for a solution to be effective. **Action:** Respect the **data minimization principle** by only collecting data that you need for each use case. This also includes using anonymized or pseudonymized data, where possible.

☐	**Take a long-term approach.** Solutions should only retain data as long as is necessary for the purposes for which it was collected. **Action**: Determine a suitable and realistic **data retention** period and ensure that data is regularly deleted once it is no longer necessary.
☐	**Ensure the security of data.** Solutions should include protections to secure any collected data. **Action**: Ensure **data security** by determining appropriate access controls and permissions on a need-to-know basis. Provide guidance and training to staff for responsible use of the product or service. Review our Security website for Salesforce best practices here.
Additional Requirements	
☐	**Think through the legal justifications for the data collection.** In Europe and other parts of the world, it is essential that you identify and document the **legal grounds** that justify the data collection. **Action**: Note that some sensitive data (such as data related to health or ethnicity) is often afforded extra protections under the law which can mean that the use of such data is prohibited unless a suitable legal exemption applies (e.g. where explicit consent is obtained or if processing the data is strictly necessary for public health reasons).
☐	**Check your contracts have the right terms.** **Action**: Work to include protective terms in the **contracts with any vendors or third parties** that will use the product or service or have access to the data contained within it. Bind them contractually to the same level of security requirements as you have imposed on your own organization and ensure the contract allows for effective oversight of these requirements.
☐	**Make sure procedures are in place to respond to data subject requests.** Many regions (including Europe and California) grant rights to individuals related to the use of their data. **Action**: Put in place, and then follow, a documented process to respond to and deal with **requests from individuals exercising their rights** with respect to the data processed as part of the product or service. This would include requests for access to the data and deletion of the data, among others.
☐	**Conduct a privacy assessment.** **Action**: Document all of the steps mentioned above and any measures taken to address them in a **Data Protection Impact Assessment**, and keep that document under review. More information on Data Protection Impact Assessments can be found on the UK Information Commissioner's Office website.
☐	**Only use the data for the purposes disclosed in your privacy notice.** **Action**: Respect the **purpose limitation principle** by ensuring that the data your organization collects through the product or service is only used for disclosed and justifiable purposes. Do not use the data for purposes other than those stated in the privacy notice.
☐	**Make sure the data is accurate.** **Action**: Ensure that the data that you collect or use in relation to your product or service is **accurate** and kept **up to date.**

☐	**Review product documentation.** **Action**: There are best practices for data storage within the product documentation, including how to limit the export of data, and placing sensitive personal data in a separate org.

Being a trusted advisor to our customers is a top priority for Salesforce. However, it remains the responsibility of each customer to get their own legal advice when implementing and using Salesforce products. It is important for customers to take into account their own particular use cases to ensure compliance with local privacy and healthcare laws, any certification requirements as well as any other applicable law or guidance.

If you have any questions about the Salesforce products, please contact your dedicated Account Executive.