Work.com Privacy FAQ
Questions and Answers for Salesforce Customers

Published: October 2020

This document provides a broad overview of some commonly raised privacy questions in connection with Work.com; it is not intended to be legal advice. Work.com provides you with essential solutions designed to help businesses reopen the workplace as quickly as possible. It also allows you to collect and use personal information about individuals, including health-related information, which is subject to various legal requirements in different jurisdictions. As with all Salesforce products, please consult with your own counsel to confirm that your intended use of these products meets your legal needs. This FAQ is provided as of the date of document publication, and may not account for changes after the date of publication.

At Salesforce, trust is our #1 value and the protection of our customers' data is paramount. In this document we have provided responses to some of the common questions that customers are asking about our Work.com solutions, particularly in response to the COVID-19 pandemic and how Salesforce addresses privacy and data protection laws generally.

1. What is Work.com?

Work.com is an all-new suite of applications and advisory resources to help business and community leaders around the world reopen safely, reskill employees and respond efficiently to the COVID-19 pandemic. Work.com brings together the full power of health experts, business leaders, Salesforce ecosystem and the world's #1 CRM Platform, to help leaders safely and responsibly manage returning to the workplace, reopen communities and prepare for a new normal.

To safely and responsibly reopen, businesses, communities and leaders need a comprehensive view of all the necessary data to make informed decisions, along with tools to help them understand individuals' health and manage wellness. Work.com addresses these needs by providing solutions to accelerate private and public sector response to the COVID-19 pandemic, ranging from manual contact tracing and emergency response management to employee wellness assessments and vaccine administration.

2. Why are privacy and data protection important when considering technological solutions to help with reopening?

Work.com relies on the use of data. Because COVID-19 is a human health crisis, much of that data is about people, and may include their health data. Because health data is often more sensitive or private in nature, it is typically offered additional protections in privacy and data protection laws.

Protecting data is also important because it helps with adoption. Businesses, public health entities, and end users (such as employees) are more willing to engage with technological solutions when they trust that their personal data is protected.

Please see Salesforce's Privacy and Ethical Use Principles Guiding our COVID-19 Response, which informs our approach to responding to the increasing and dynamic COVID-19 challenges and needs.

3. Is Work.com compliant with privacy laws?

The security and privacy of our customers' data is paramount. Salesforce has five privacy principles that highlight our commitment to trust: customer control, security, transparency, compliance, and partnership. Salesforce has robust and comprehensive privacy and security programs addressing the use, disclosure, and protection of our customers' data, including sensitive data like employees' health information. Our commitments to customer privacy and security are described in our Data Processing Addendum, which is part of our contract with our customers.

Salesforce designs its products with privacy in mind, not only to ensure compliance with our legal obligations, but so our customers can meet their own legal obligations when using our products. However, compliance is always a shared partnership between Salesforce and our customers, meaning that customers are responsible for ensuring that their use of our products is appropriate for their own legal requirements. COVID-19 is an example of this: customers will face different issues depending on their businesses, the jurisdictions where they operate, and the ways in which they choose to use our services. A government agency may have different legal powers than a private company, and may face very different challenges, and a "one size fits all" approach to legal compliance will not work. For that reason, we encourage you to get your own legal advice when implementing and using Salesforce products, including Work.com, to ensure compliance with local healthcare laws, certification requirements, and any other applicable laws or guidance.

To act as a trusted advisor and help customers meet their compliance goals, we have created a number of dedicated resources for customers to learn more about privacy obligations, such as Salesforce's privacy website, which includes FAQs on local and industry specific privacy laws, and additional resources, such as a Data Protection Impact Assessment. We hope that these resources will help enable your success.

4. How does Work.com secure customers' data?

Salesforce has implemented default technical and administrative security measures to protect our services and our customers' data. We also strongly encourage customers to follow security best practices and to use the configurable security controls we offer to further strengthen the security of their Salesforce instances. Customers can use these controls to add protections appropriate to the sensitivity of their data, including Field Level Security, Profiles and Permission Sets, Two Factor Authentication and IP safelists. For more information on the application security features Salesforce provides, please refer to this help article on Protecting Your Salesforce Organization.

In addition, our Compliance website details our audit and compliance certifications and attestations, and our Trust website shows real-time information on system performance and security. Contractually, our Data Processing Addendum commits to maintain appropriate technical and organizational measures to

protect our customers' data, as detailed in each service's Security, Privacy and Architecture Documentation.

5. What should be considered when using Work.com in the US, and in particular, when considering the Health Insurance Portability and Accountability Act (HIPAA), the Americans with Disabilities Act (ADA), and the Family Educational Rights and Privacy Act (FERPA)?

The US has different laws that regulate the processing of health data, including data about employees' and students' health and wellness. HIPAA governs the use and disclosure of health data in certain circumstances in the US, but not all circumstances. For example, HIPAA generally would govern the collection and use of individuals' health data by healthcare organizations when providing healthcare services to those individuals as part of a vaccine administration program that is managed using Work.com for Vaccines.

In contrast, HIPAA generally does not apply to employers that collect health information from their employees. Rather, in the US, the ADA is the federal law that regulates how and when employers may request health information from their employees. Similarly, HIPAA generally does not apply to educational institutions that collect health information from their students. Rather, the Family Educational Rights and Privacy Act (FERPA) is the federal law that regulates how and when institutions may request, use, and disclose health information from or about their students.

Under ADA regulatory guidance, employers are permitted to ask more detailed questions about employees' COVID-19-related health status because the disease has been declared a pandemic and can threaten employees' health and safety. To comply with the ADA, employers must still ensure that health information collected from employees is maintained in separate, confidential records where access is limited to authorized personnel for permitted purposes only. Customers can configure Work.com solutions to help meet these requirements, including by setting access controls so that only authorized personnel can view employees' sensitive health data.

Under the US Department of Education's guidance, a parent or eligible student must generally provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from a student's education records, including student health records, unless an exception applies. Customers can configure Work.com solutions to support these requirements, by leveraging the pre-configured consent mechanism within Wellness Check and setting all data access permissions on the platform in accordance with employee roles and responsibilities.

For more information about Salesforce and our commitments related to HIPAA, check out our HIPAA FAQ.

As with all Salesforce products, customers should consult with your own counsel to confirm that your intended use of any Work.com solutions, including Work.com for Vaccines, meets your legal needs, such as those you may have under HIPAA, the ADA or FERPA.

6. What should be considered when using Work.com in Europe, and in particular, does the General Data Protection Regulation (GDPR) require specific treatment of sensitive data and/or for European personal data to remain in Europe?

Sensitive Data

The GDPR states that some types of personal data merit special protection because their use could create significant risks to individuals' fundamental rights and freedoms; the GDPR refers to these data

types as special categories of personal data. Special categories include data about an individual's race; ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where this is used for identification purposes); health data; sex life; or sexual orientation.

Transfer of personal data outside of Europe

The GDPR does not require personal data to remain in Europe, including special categories of personal data. Instead, it provides a number of transfer mechanisms that allow companies and public health entities to safely and legally transfer data out of Europe. We enable our customers to comply with the GDPR's data transfer mechanisms requirements by offering a Data Processing Addendum that incorporates two transfer mechanisms: our processor Binding Corporate and the Standard Contractual Clauses as approved by the European Commission. For further information on the GDPR, its applicability, and Salesforce's role as a data processor to our customers, please see the European section and resources of our privacy website.

7. How does the Work.com manual Contact Tracing solution work? Does this solution require the collection of sensitive or special categories of personal data?

Contact Tracing helps contact tracers identify situations that pose a high risk of infectious disease transmission, and monitor the health of individuals that may have been infected. Using interview templates, contact tracers manually collect data in interviews with individuals who are infected, or who were potentially exposed to infection. Contract tracers can use this information to take steps to protect both individuals and the wider community, like tracking infections; notifying people who were in contact with an infected person; asking people with exposure to isolate; and providing guidance to exposed individuals.

The data collected will depend on the questions asked during these interviews, but will involve the collection of some personal health data, which is generally considered to be sensitive data and is a special category of personal data under the GDPR. Customizable interview templates are provided within Work.com. Depending on your needs and any legal restrictions in your jurisdiction, you may choose to replace the default interview questions with others, or to forego the use of this feature.

8. What is the Work.com Wellness Check? Does it require the collection of sensitive or special categories of personal data?

With the Work.com Wellness Check, organizations can survey employees to assess their suitability to return to work. The Wellness Check can be used to collect simple availability status from employees, or to collect sensitive or special categories of personal data, like health data, depending on how the customer chooses to use this feature. The survey questions are customizable; depending on your needs and any legal restrictions in your jurisdiction, you may choose to replace these questions with others, or to forego the use of this feature.

The Wellness Check is a part of the Workplace Command Center, from which executives and leaders can assess wellness trends to uncover insights, allowing them to make informed decisions about returning employees to the office.

Additional Resources:

Privacy website
General White Paper - GDPR and Data Protection Impact Assessments FAQ
International Data Transfers FAQ
Data Privacy and Protection Help and Training Documentation
Trust and Compliance Documentation

Cybersecurity Trailhead Module
Responsible Creation of Artificial Intelligence Trailhead
European Law Privacy Basics Trailhead
Responsible Creation of Artificial Intelligence Trailhead
US Privacy Law Basics Trailhead