Insights, News & Events

E.U. AND U.S. AGREE TO DATA PRIVACY DEAL, FREEING WAY FOR TRANS-ATLANTIC DATA SHARING: YOUR 3-STEP ACTION PLAN

Insights
Jul 13, 2023

The European Commission just adopted its adequacy decision on data transfers between the European Union and the United States, paving the path for companies to transfer data freely across the Atlantic and ending several years of confusion and delay. The newly adopted EU-U.S. Data Privacy Framework serves as a long-awaited facilitator for an easy flow of data between the U.S. and Europe. What does your business need to know about this long-awaited July 10 announcement and what three things should you do?

American Companies Had Been in a Bind

The U.S. is not one of the countries that had received an adequacy decision from the European Commission when it came to the transfer of data. Instead, American companies had relied on an alternative mechanism – the E.U.-U.S. Privacy Shield – to transfer personal data relatively freely.

However, the Shield was deemed invalid by the Court of Justice of the European Union in 2020. In the last three years, many companies have found the trans-Atlantic transfer of data challenging and felt in a sort of legal limbo given the uncertainty. Luckily, this week's decision puts companies on much better footing and provides a security blanket for data transfers between continents.

E.U.-U.S. Framework, in a Nutshell

Under the July 10 decision, the European Commission (EC) notes that the U.S. now ensures an adequate level of protection for personal data transferred from the E.U. to

Related People

Nan Sato, CIPP/E, CIPP/C
Partner
610.230.2148

Service Focus

International

Privacy and Cyber

American organizations that certified compliance to the "EU-U.S. Data Privacy Framework Principles" and are added to the Data Privacy Framework List maintained by the U.S. Department of Commerce.

While the Framework is subject to periodic reviews by the EC, representatives of European data protection authorities, and competent U.S. authorities, it now provides a stable means by which organizations can feel confident when it comes to trans-Atlantic data sharing.

More expansive than the previous Privacy Shield, the EC notes that the Framework has new binding safeguards, including limiting access to EU data by US intelligence services to what is necessary and proportionate.

It also establishes a Data Protection Review Court (DPRC) to which EU individuals will have access. If the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

The new safeguards in the area of government access to data will complement the obligations that American companies importing data from EU will have to subscribe to.

American companies can now self-certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. These include an updated, more substantial version of the principles established under the Privacy Shield framework.

3 Steps for U.S. Companies

If you are an American organization seeking to benefit from this new policy, we suggest you follow the following three steps:

1. Apply to the U.S. Department of Commerce (DOC) to be added to the Data Privacy Framework List. This will require you to self-certify your adherence to the E.U.-U.S. Data Privacy Framework Principles.

2. Begin collecting information that will be required for the self-certification process. Types of information required can be found on the International Trade Commission DPF Overview Website.

3. Review your privacy policy to check accuracy and compliance with the framework.

Conclusion

We will continue to monitor these developments and provide updates as warranted. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. For additional information about compliance, or if your organization needs to transfer personal data from the E.U. to the U.S., contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Practice Group or International Practice Group.