



How U.S. Businesses Can Freely Transfer Personal Data of EU Residents to the U.S.

Article

08.25.2023

Many U.S. businesses have had to use the rather complex and confusing Standard Contractual Clauses (“SCC”) to transfer personal data of EU residents to the U.S. Now, however, there is another and more streamlined way to transfer personal data of EU residents to the U.S.

On July 10, 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework (the “Framework”). In effect, the European Commission concluded that, through compliance with the Principles in the Framework, U.S. businesses ensure comparable protection of personal data to the protections under the General Data Protection Regulation (GDPR).

Businesses can take advantage of the benefits of the Framework by complying with the Principles and Supplemental Principles (as applicable) in the Framework and submitting a self-certification to the U.S. Department of Commerce of compliance.

If a business maintained its certification under the former EU-U.S. Privacy Shield (the “Privacy Shield”), then that certification may be used as a certification under the Framework. This is because, after the Privacy Shield was deemed not adequate, the U.S. government needed to adopt additional security mechanisms on its side, which it did in October of 2022.

Self-certification includes seven (7) primary Principles, as well as other Supplemental Principles addressing particular circumstances. The 7 primary Principles are:

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

How U.S. Businesses Can Freely Transfer Personal Data of EU Residents to the U.S.

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement, and Liability

The Supplemental Principles address areas such as treatment of sensitive data, verification, access, human resources data, opt-out, and other particular situations that arise in the processing of personal data.

To take advantage of the ease of transfer under the Framework, businesses must self-certify to the U.S. Department of Commerce regarding their adherence to the Principles and Supplemental Principles, as applicable. Self-certification includes:

- Name of organization, mailing address, e-mail address, telephone, and fax numbers;
- Description of the activities of the organization with respect to personal data received from the EU; and
- Description of the organization's privacy policy for such personal data, including:
 - If the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;
 - Its effective date of implementation;
 - A contact office for the handling of complaints, access requests, and any other issues arising under the Framework;
 - The specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy;
 - Name of any privacy program in which the organization is a member;
 - Method of verification (e.g., in-house, third party); and
 - The independent recourse mechanism that is available to investigate unresolved complaints.
- Where the organization wants the Framework benefits to cover human resources information transferred from the EU for use in the context of the employment relationship:
 - The organization may do so where a statutory body listed in the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information;
 - In addition, the organization must indicate this in its self-certification submission and declare its commitment to cooperate with the applicable EU authority or authorities in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities,

How U.S. Businesses Can Freely Transfer Personal Data of EU Residents to the U.S.

as applicable, and that it will comply with the advice given by such authorities;

- The organization must also provide the U.S. Department of Commerce with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

If your business is trying to address how to properly transfer personal data from the EU to the U.S. and would like to learn more about the EU-U.S. Privacy Framework, meeting the Principles, and self-certification, Burr & Forman's Cybersecurity & Data Privacy Team can help.