Guidepost

NEW EU-U.S. DATA PRIVACY FRAMEWORK LEGALIZES PERSONAL DATA TRANSFERS FROM THE EU TO US

What happened?

On July 10, 2023, the European Commission announced that it had adopted its adequacy decision for the EU-U.S. Data Privacy Framework (EU-U.S. DPF). This long-awaited decision means that for the first time since the EU-U.S Privacy Shield was invalidated nearly three years ago (and other transfer mechanisms were called into question), there is a clearly established mechanism to transfer personal data from the EU to U.S. companies in compliance with the EU's General Data Protection Regulation (GDPR).

How did we get here?

GDPR (and before that, the EU Data Protection Directive) strictly limited transfers of personal information from within the EU to countries outside of the EU unless the European Commission determines that the non-EU country ensures "an adequate level of protection" which is effectively equivalent to the level of protection within the EU. The first mechanism to accomplish this was the "Safe Harbor Privacy Principles" framework which received an adequacy decision almost 23 years ago in July of 2000. Safe Harbor was challenged by privacy rights activist Maximilian Schrems in 2013, and was invalidated in July 2015 by the European Court of Justice (in a case known as Schrems I), in a decision which among other things cited a lack of applicability of the Safe Harbor principles to U.S. government authorities.

The European Commission then replaced Safe Harbor one year later with the somewhat more robust EU-U.S. Privacy Shield framework in July 2016. Some companies also began, or had already been, relying on another older and more complicated transfer mechanism called "standard contractual clauses" (SCCs). These SCCs were also accepted as GDPR compliant at the time, having been first approved by the EU Parliament in 1995, and having received an adequacy decision adopted by the European Commission in 2001. The SCCs were challenged by Maximilian Schrems in 2015 (in a case known as Schrems II) and ultimately the European Court of Justice considered both the SCCs as well as the EU-U.S. Privacy Shield (the latter having received its adequacy decision subsequent to the filing of Schrems II). The

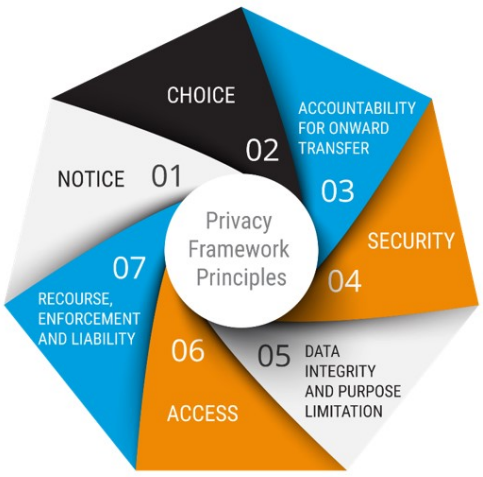
European Court of Justice decision invalidated EU-U.S. Privacy Shield entirely, for reasons including a lack of actionable rights for individuals to challenge the actions of U.S. authorities before the courts.

SCCs were not completely invalidated, but the Court of Justice did hold that the SCCs must incorporate specific provisions addressing access by the public authorities of the destination country to the data transferred as well as the relevant aspects of the legal system. The SCCs were later updated to attempt to address this ruling. In practice, however, there are substantial challenges to implementing such provisions, as illustrated by a recent case where Meta was fined $1.3 billion for EU/U.S. transfers carried out on the basis of standard contractual clauses. In that case, the European Data Protection Board ruled that "the [organizational], technical and legal measures implemented by Meta IE…[cannot] compensate for the deficiencies identified in U.S. law and cannot provide essentially equivalent protection to that available under EU law."

What does the recently adopted EU-U.S. Data Privacy Framework mean for U.S. Companies?

U.S. companies and organizations (as well as European subsidiaries and other entities) will be able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards (e.g., SCCs) and/or risking non-compliance with the GDPR. They will first need to join EU-U.S. DPF by self-certifying their adherence to a detailed set of privacy framework principles (Principles) issued by the U.S. Department of Commerce. These Principles may include (but are not necessarily limited to) the following:

- NOTICE



U.S. companies or organizations must provide a clear and conspicuous privacy notice containing 14 separate information points to individuals at the time of collection of personal information. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party. The notice provided by the U.S. company or organization must inform individuals about:

- Its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List (of participating organizations)
- The types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization also adhering to the Principles
- Its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF
- The purposes for which it collects and uses personal information about them
- How to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints
- The type or identity of third parties to which it discloses personal information, and the purposes for which it does so
- The right of individuals to access their personal data
- The choices and means the organization offers individuals
- The choices and means the organization offers or limiting the use and disclosure of their personal data
- The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States
- Being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body
- The possibility, under certain conditions, for the individual to invoke binding arbitration
- The requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements
- Its liability in cases of onward transfers to third parties

- CHOICE

An organization must offer individuals clear, conspicuous, and readily available mechanisms to exercise choice (i.e., opt out), and express consent (i.e., opt in) for sensitive data, as to whether their personal information is disclosed to a third party or used for a purpose other than those for which it was originally collected.

- ACCOUNTABILITY FOR ONWARD TRANSFER
    - To transfer personal information to a third party acting as a controller, organizations must:
        - Comply with the Notice and Choice Principles.
        - Enter into a contract with the third-party controller that among other required elements, provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles
    - To transfer personal data to a third party acting as an agent, organizations must, among other requirements:
        - Transfer such data only for limited and specified purposes
        - Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles
        - Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles;

- SECURITY

Organizations creating, maintaining, using, or disseminating personal information must implement reasonable security to protect and ensure availability of that information.

- DATA INTEGRITY AND PURPOSE LIMITATION

Personal information collection, processing and retention must be limited to the information that is relevant and necessary for the purposes of processing.

- ACCESS

Subject to some exceptions, individuals must be provided access to personal information about them that an organization holds and be able to correct, amend, or delete that information as required. Access must be provided "…within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual."

- RECOURSE, ENFORCEMENT AND LIABILITY

Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed.

What are the consequences of non-compliance?

Failure to adhere to the EU-U.S. DPF Principles by U.S. companies or organizations which have self-certified, or otherwise held themselves out to the public as complying with the Principles, may trigger regulatory enforcement and significant fines and penalties, as well as civil litigation. Under the prior Privacy Shield and Safe Harbor frameworks, the Federal Trade Commission took law enforcement action against dozens of companies that made false or deceptive representations about participation in those frameworks using its authority under the Federal Trade Commission Act.

Companies found to be persistently out of compliance with the EU-U.S. DPF are likely to be removed or barred from by the EU-U.S. DPF list maintained by the Department of Commerce and would then be required to return or delete the personal information they received under the EU-U.S. DPF. In addition, there is potential for significant fines and penalties resulting from enforcement by the FTC under Section 5 of the Federal Trade Commission (FTC) Act prohibiting unfair or deceptive acts in or affecting commerce (15 U.S.C. § 45); enforcement is also possible by the DOT under 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice. Accordingly, companies participating in the EU-U.S. DPF should have strong documentation of their compliance with the EU-U.S. DPF Principles and be prepared to evidence that compliance to regulators.

What's next?

It should be noted that the new EU-U.S. DPF is the *third* attempt (or the fourth, if you count the SCCs) to address the requirements of EU privacy law and allow for the safe flow of personal data from the EU to the U.S. It is designed to address the past findings of the European Court of Justice, such as by limiting access by U.S. public authorities to in scope data which is necessary and proportionate to protect national security, and by providing impacted individuals an independent and impartial redress mechanism regarding the collection and use of their data by U.S. intelligence agencies.

However, just as with the prior frameworks, the adequacy of EU-U.S. DPF and these mechanisms is certain to be challenged in the EU courts (Schrems III?). It is entirely possible that the EU-U.S. DPF may not survive these challenges, and that SCCs may also prove difficult for many companies to implement without risk of significant regulatory scrutiny. These companies should carefully consider alternatives to EU-U.S. data transfers, such as data localization within the EU, or additional technical safeguards for access to data that is transferred to the U.S. which require approval of managers within the EU.

A cookie-cutter approach is also unlikely to be effective; compliance with EU-U.S. DPF will require that the myriad of context variables in each company's data sets and use cases be reviewed by a privacy subject matter expert to determine overall compliance strategy, content and elements of the company's privacy notice and data processing agreements, as well as other applicable requirements. A program to allow exercise of consumer and individual privacy rights must also be built and implemented. Companies may also benefit from assistance with project planning and implementation via a third-party consultant with experience in efficient risk-based privacy program design and in avoiding the common pitfalls inherent in building these types of programs.

MATTHEW CORWIN CISA, CISSP, CDPSE

Managing Director

Matthew A. Corwin has more than 20 years of experience specializing in privacy, regulatory compliance, and cybersecurity with specialized hands-on experience directing the implementation and integration of secure design principles and service engineering initiatives leveraging the latest technologies. He has a successful track record of facilitating technology-business alignment while balancing risk exposure and corporate growth. Mr. Corwin also has extensive expertise in analyzing technical architecture to attain and demonstrate best-in-class industry and regulatory standards compliance in global environments.