

## **EU–US Privacy Shield Approved to Replace Safe Harbor**

Article By:

Pulina Whitaker

Gregory T. Parks

W. Reece Hirsch

Mark L. Krotoski

---

**The EU-US Privacy Shield—successor to the invalidated Safe Harbor program for transatlantic transfers of EU personal data—was finally approved on July 12, 2016.**

US organizations will be able to certify compliance with the Privacy Shield principles starting on August 1, 2016, and thereafter be able to receive personal data from EU-based organizations without specific consent or special agreements in place with the EU data exporters. This option will be welcomed by thousands of US organizations that had previously been Safe Harbor-certified.

Although the first draft of the EU-US Privacy Shield was heavily criticized for failing to include sufficient safeguards for the privacy of EU personal data in the hands of US organizations (and, potentially, the US government or US law enforcement), European Commissioners Andrus Ansip and Věra Jourová have declared that it is “fundamentally different from the old Safe Harbor; it imposes clear and strong obligations on companies handling the data and makes sure that these rules are followed and enforced in practice.”

There does, however, remain an ongoing concern of legal challenges similar to the challenge that invalidated the Safe Harbor framework and, more recently, against the use of EU model clauses.

### **Safe Harbor Invalidated**

According to the European Commission, the US is a country with “inadequate” data protection laws. As a result, a company cannot transfer personal information from Europe to the US unless the company has implemented one of the approved data transfer mechanisms. In 2000, the European Commission and the US Department of Commerce agreed to implement a self-certification program for US organizations to receive personal data sent from Europe whereby US organizations certified adherence to certain standards of data processing comparable to EU data protection laws such that EU citizens’ personal data was treated as adequately as if it had remained within Europe.

The Safe Harbor program was invalidated by the European Court of Justice (ECJ) in October 2015.<sup>[1]</sup> Further, the ECJ ruled that EU data protection authorities (DPAs) can investigate complaints about the transfer of personal data outside Europe and, where necessary, suspend such data transfers until those investigations are satisfactorily completed. The ECJ also found that EU citizens do not have adequate rights of redress where their personal data protection rights are breached by US authorities, which undermines their European data protection rights.

## Proposed Privacy Shield

On February 29, 2016, the European Commission published a draft adequacy decision to establish the EU-US Privacy Shield as the replacement for the invalidated Safe Harbor program. The EU-US Privacy Shield would be operated by the US Department of Commerce and enforced by the US Federal Trade Commission, as was the Safe Harbor program.<sup>[2]</sup>

The publication of the draft adequacy decision was initially welcomed by the Article 29 Working Party (Article 29 WP), the body advising the European Commission on privacy matters. Following a review of the documentation, however, the Article 29 WP expressed significant concerns that the draft proposal did not give enough protection to European citizens because “. . .massive and indiscriminate data collection is not fully excluded by the US authorities and. . .the powers and position of the Ombudsman have not been set out in more detail.”<sup>[3]</sup>

## Approved Privacy Shield

The decision approving the Privacy Shield was released on July 12, 2016. The Privacy Shield will be in force immediately, and US organizations will be able to certify compliance with its principles starting on August 1, 2016.

The key principles of the Privacy Shield are the following:

- Strong obligations on companies handling data. Under the new arrangement, the US Department of Commerce will conduct regular updates and reviews of participating companies to ensure that they follow the rules and that onward transfers are protected to the same levels of protection.
- Clear safeguards and transparency obligations on US government access. The United States has given the European Union assurances that the access of public authorities for law enforcement and national security purposes is subject to clear limitations, safeguards, and oversight mechanisms. EU residents will, for the first time, benefit from redress mechanisms in this area. The US has ruled out indiscriminate mass surveillance on personal data transferred to the US under the Privacy Shield arrangement. The US Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. The US Secretary of State has established a redress possibility in the area of national intelligence for EU residents through an Ombudsman mechanism within the US Department of State.
- Effective protection of individual rights. Any EU resident who considers that his or her data has been misused under the Privacy Shield scheme will benefit from several accessible and affordable dispute resolution mechanisms. Ideally, the complaint will be resolved by the company itself or through the Alternative Dispute Resolution solution offered by the company. Individuals can also lodge complaints with their national DPA, which will work with the Federal

---

Trade Commission to ensure that complaints are investigated and resolved. If a case is not resolved by any of the other means, there will be an arbitration mechanism to serve as a last resort. National intelligence matters will be resolved by the Ombudsman.

- Annual joint review mechanism. This mechanism will monitor the functioning of the Privacy Shield. The European Commission and the US Department of Commerce will conduct the review in association with national intelligence experts from the US and the European DPAs. The European Commission will draw on all other sources of information available and will issue a public report to the European Parliament and the European Council.

## Alternative EU-US Data Transfers

There are other options to transfer personal data to the US, including express consent and the use of Binding Corporate Rules or EU-approved model clause agreements. Model clauses are very commonly used. Other than in a few European countries, there is no requirement to obtain a specific permit from the applicable DPA to use model clause agreements. The use of model clauses, however, has been recently challenged by Maximilian Schrems<sup>[4]</sup> in new legal proceedings that have been referred to the ECJ by the Irish DPA. Mr. Schrems has also indicated that he may bring proceedings charging that the Privacy Shield does not adequately protect personal data.

## Brexit Implications

Following the United Kingdom's referendum decision to leave the European Union, for now, the Privacy Shield will be effective for data transfers from the UK to US certified organizations. If and when the UK's new prime minister, Theresa May, elects to invoke Article 50 of the Lisbon Treaty (triggering an exit from the European Union), trade negotiations will commence to secure the UK's ability to trade with the remainder of the EU as a single market. Most UK businesses will almost certainly need to transfer personal data to Europe and other countries outside the EU, such as the US.

While the UK remains part of the EU, the Privacy Shield will apply, as will the general restriction against transferring personal data outside the UK. If the UK does leave the EU, the UK government will need to decide if it will retain the same restrictions for cross-border transfers or adopt an alternative solution, such as a potential UK-US Privacy Shield. In this event, the UK government will need to reassure the European Commission (as the US government has now done) that it will limit mass surveillance and bulk data collection. This is already a contentious issue under the UK Telecommunications Act 1984 and the draft Communications Data bill currently making its way through Parliament.

---

[1] See, "[ECJ Rules EU-US Safe Harbor Programme Is Invalid.](#)"

[2] See, "[EU-US Privacy Shield to Replace Safe Harbor.](#)"

[3] See, "[Article 29 Working Party Expresses Concerns About EU-US Privacy Shield.](#)"

[4] Austrian privacy activist who prevailed in Schrems v. Data Protection Commissioner, resulting in the the invalidation of the Safe Harbor program.

National Law Review, Volume VI, Number 194

Source URL: <https://natlawreview.com/article/eu-us-privacy-shield-approved-to-replace-safe-harbor>