On February 2, 2016, the European Commission (EC) and the U.S. Department of Commerce (Commerce) announced that they had reached agreement on a new data transfer safe harbor arrangement for the transfer of personal data from Europe to the U.S. The new safe harbor pact, called the EU-US Privacy Shield, was negotiated in the wake of the EU Court of Justice’s (CJEU) decision in October 2015 invalidating the prior safe harbor for transfers of personal data to the U.S. However, the details of the EU-US Privacy Shield still must be formalized for it to go into effect, and it remains subject to the scrutiny of the official consortium of EU data protection authorities known as the Article 29 Working Party. The opinion of the Article 29 Working Party, which is expected in April of this year, likely will strongly influence whether or not the EU-US Privacy Shield will be formally approved and implemented by EU authorities.

Background

Under the EU’s Data Protection Directive (Directive 95/46/EC), personal data may be transferred from the EU to a country outside of the EU only if the non-EU country ensures an adequate level of protection of the personal data. In determining whether a non-EU country provides adequate protections, consideration is given to, among other things, the adequacy of the data privacy and security laws and regulations in force in the non-EU country. Article 25(6) of the EU Data Protection Directive enables the EC to make a finding that a non-EU country “ensures an adequate level of protection...by reason of its domestic law or of the international commitments it has entered into.” Under Article 26(4) of the EU Data Protection Directive, the EC has also approved standard (model) contract clauses to allow parties that adopt the model clauses to transfer personal data to a non-EU country.

Prior to the CJEU decision in October 2015, parties could comply with the EU Data Protection Directive for transfers of personal data from the EU to the U.S. under any of the following three alternatives:

(i) **Model Contract Clauses**: The parties could enter into contracts with model clauses for data transfers that have been approved by the EC pursuant to Article 26(4) of the EU Data Protection Directive. This alternative would work for transfers between third parties or for transfers within a multinational group of companies;

(ii) **Binding Corporate Rules (BCRs)**: For internal data transfers within a multinational group of companies, the company group could adopt BCRs that were approved by the applicable EU data protection authorities; and

(iii) **Prior EU-US Safe Harbor**: Data transfers could be made to U.S. companies that self-certified compliance with certain safe harbor principles.

Contacts

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed or the Sutherland attorney with whom you regularly work.

Brian M. Murphy
Partner
brian.murphy@sutherland.com
404.853.8178

Mary Jane Wilson-Bilik
Partner
mj.wilson-bilik@sutherland.com
202.383.0660

Mark Thibodeaux
mark.thibodeaux@sutherland.com
713.470.6104

Related People/Contributors

- Mark D. Herlach
- Brian M. Murphy
- Robert D. Owen
- Robert J. Pile
- Mary Jane Wilson-Bilik
- Mark Thibodeaux
Legal Alert: EU-US Privacy Shield: European Union and U.S. Reach Agreement in Principle for New Data Transfer Framework – But Uncertainty Remains continued

under the EC’s Decision 2000/520, which was adopted by the EC pursuant to Article 25(6) of the EU Data Protection Directive.

However, in the landmark decision, Maximillian Schrems v. Data Protection Commissioner, the CJEU invalidated the EU/US safe harbor under Decision 2000/520. After 15 years of reliance on the old safe harbor, the court’s judgment has left many EU and U.S. companies scrambling to put in place alternative measures to permit the continued lawful transfer of personal data from the EU to U.S. companies. Further, the EU’s Article 29 Working Party has indicated that it is reevaluating personal data transfers to the U.S. under model contract clauses and BCRs in light of the Schrems ruling.3

The CJEU rendered its judgment in Schrems to invalidate the old EU/US data transfer safe harbor, in part, on the basis that Decision 2000/520 permitted U.S. authorities and companies to limit adherence to the safe harbor principles (i) to the extent necessary to meet national security, public interest or law enforcement requirements, and (ii) pursuant to conflicting U.S. laws or regulations. Thus the court found that Decision 2000/520 gave national security, public interest or law enforcement requirements primacy over the safe harbor principles, such that U.S. intelligence and law enforcement authorities were able to access Europeans’ personal data and “process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security.”4 The court also found that European data subjects had no administrative or judicial means of redress with respect to complaints about how their data was being treated in the U.S. The court’s decision was rendered following the disclosure by Edward Snowden of U.S. intelligence surveillance programs such as the National Security Agency’s PRISM program, and the court and EU authorities were particularly concerned about generalized mass surveillance programs brought to light by the Snowden leaks.

EU-US Privacy Shield

Following the Schrems decision, the EU’s Article 29 Working Party established a deadline of January 31, 2016 for the EC and the U.S. to reach agreement on a new safe harbor framework that addressed the concerns set forth in the CJEU’s decision.5 The EC and Commerce announced agreement on the new EU-US Privacy Shield safe harbor framework just two days after the deadline set by the Article 29 Working Party, and described the following key elements of the EU-US Privacy Shield agreement:

- **Stronger obligations on U.S. companies:** U.S. companies will be required to commit to “robust obligations” on how they will process personal data to guarantee individual rights and will be required to publish these commitments.

- **More robust enforcement:** The U.S. Federal Trade Commission (FTC) will continue to serve a lead enforcement role in the event companies fail to adhere to their commitments under the new safe harbor. Commerce will also
perform a monitoring and enforcement role under the EU-US Privacy Shield.

- **Clear and transparent safeguards and obligations on access to personal data by U.S. authorities**: The U.S. has given the EU assurances that access to personal data by U.S. authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. Exceptions to the new safe harbor principles must be used only to the extent necessary and proportionate. According to the EC, the U.S. has ruled out indiscriminate mass surveillance on Europeans’ personal data that is transferred to the U.S.

- **Increased cooperation**: The EU and U.S. have committed to improved cooperation between the FTC and Commerce on the one hand and EU data protection authorities on the other hand with respect to referral of complaints by EU data subjects and enforcement actions.

- **Regular reviews**: The EC, Commerce and the FTC will conduct joint annual reviews of the new safe harbor framework to assess its effectiveness and to make changes as necessary. According to the EC, these reviews will specifically include the scope of national security access to personal data by U.S. authorities.

- **Increased avenues for redress**: European citizens who believe that their data has been misused under the new safe harbor framework will have several avenues for redress, including (i) deadlines for companies to reply to complaints, (ii) increased cooperation with respect to referral of complaints by European data protection authorities to Commerce and the FTC, (iii) alternative dispute resolution that will be free of charge to data subjects, and (iv) creation of a new dedicated ombudsperson to whom Europeans can raise enquiries and complaints.

### Next Steps for the EU-US Privacy Shield

The EU-US Privacy Shield safe harbor will not take effect until the EC adopts a formal Decision that sets forth the details of how the new safe harbor framework will work. In the meantime, the EU’s Article 29 Working Party has requested that the EC provide it with all documentation related to the EU-US Privacy Shield arrangement by the end of February. The Article 29 Working Party has said that it aims to issue an opinion on the arrangement by April 2016.

The Article 29 Working Party has identified the following four essential guarantees for intelligence activities that will likely factor strongly in its assessment of the proposed EU-US Privacy Shield safe harbor: (i) clear, precise and accessible rules so that a reasonably informed person can foresee what might happen with his or her data; (ii) demonstration of necessity and proportionality to strike a balance between the needs of national security and the rights of the individual; (iii) presence of an independent and effective oversight mechanism; and (iv) effective remedies
available to individual data subjects. If the Article 29 Working Party renders a favorable opinion of the EU-US Privacy Shield deal, then the EC should be able to approve a Decision to implement the new safe harbor framework. However, if the Article 29 Working Party objects to the new framework, formal approval by the EC is questionable, and the EU and U.S. may then need to restart negotiations.

The Article 29 Working Party has also cast a pall of uncertainty on the future use of model contract clauses and BCRs for personal data transfers to the U.S. with its announcement of plans to review the efficacy of these alternatives in light of the Schrems decision. However, the Article 29 Working Party has indicated that for now model clauses and BCRs can still be used.

The U.S. will also have some legwork to do to put in place the safe harbor principles and procedures for improved cooperation with EU data protection authorities under the EU-US Privacy Shield. The FTC will continue to serve as the lead enforcement agency for compliance by U.S. companies under the new arrangement. According to FTC Commissioner Julie Brill, not much is expected to change in terms of the FTC’s enforcement role, but it will need to improve on how it cooperates with EU authorities on enforcement matters. Commissioner Brill also stated that the FTC will strongly enforce entities that self-certify that they will be part of the EU-US Privacy Shield, suggesting that the new framework will carry over self-certification as the mechanism by which U.S. companies come within the fold of the new EU-US Privacy Shield safe harbor, similar to the process under the old safe harbor framework. Commerce will also play a leading role with respect to monitoring the EU-US Privacy Shield and cooperation with EU authorities for complaint referrals. Commerce has stated that it will dedicate a special team with significant new resources to this effort.

In the meantime, on February 10, the U.S. House of Representatives passed the version of the Judicial Redress Act of 2015 (H.R. 1428) already approved by the Senate, which was seen by many as essential to getting the EU to adopt a formal agreement for a new data transfer safe harbor. The bill would extend the rights of U.S. citizens to citizens of certain countries designated by the U.S. Department of Justice, which presumably would include EU countries, to bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending or redressing unlawful disclosures of records transferred from a foreign country to the U.S. for law enforcement purposes. The bill remains subject to the President’s signature before becoming law.

**What This Means for EU and U.S. Companies**

There is still a fair amount of uncertainty about how the EU-US Privacy Shield safe harbor will work or if it will even be formally approved by the EC. EU and U.S. companies should keep an eye out for the Article 29 Working Party’s opinion expected in April 2016, which should shed considerable light on whether or not the EU-US Privacy Shield will be implemented as the new data transfer safe harbor. What is certain, however, is that following the Schrems decision, currently there is
no safe harbor in effect for the transfer of personal data from the EU to the U.S. Therefore EU and U.S. companies should immediately put in place alternative mechanisms, such as model contracts or BCRs, to permit personal data transfers from the EU to the U.S. for now.

1 The Article 29 Working Party is composed of representatives from each EU country, as well as a representative of the EC and of the EU institutions.

2 Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (October 6, 2015) (holding that the U.S. did not ensure an adequate level of protection of personal data when an Austrian citizen’s Facebook data was transferred from Facebook’s Irish subsidiary to servers located in the U.S.).


4 See Schrems.


7 Id.

8 5 U.S.C.A. § 552a

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed under ‘Related People/Contributors’ or the Sutherland attorney with whom you regularly work.