Transatlantic Data Flows Still on the Brink: New EU-U.S. Agreement Creates Further Uncertainty

By Anahita Thoms and Christoph Werkmeister

Introduction

In October 2015, the European Union Court of Justice (CJEU) found the European Union-U.S. Safe Harbor Framework, which let European Union businesses transfer personal data to self-certified U.S. businesses, to be invalid.1 Although the ruling, in its essence, only concerns transnational data flows that solely rely on the Safe Harbor framework, it has opened a Pandora’s box: now any data flow from the EU to the U.S., even if it is grounded on other legal bases than Safe Harbor, is being called into question. Policy makers in the EU and the U.S. reacted quickly by speeding up talks to negotiate a successor to Safe Harbor, also referred to as “Safe Harbor 2.0.” On 2 Feb., 2016, the European Commission finally announced that the parties had come to a new agreement, the “Privacy Shield,” that is supposed to be as robust as Safe Harbor and will allow European Union businesses to transfer personal data from the EU to the U.S. without going through the lengthy and expensive transatlantic negotiations. However, there are no concrete details on the new deal yet, and it remains to be seen whether the new Privacy Shield will live up to its expectations.

1 Cf. case C-362/14 - Schrems (6 Oct. 2015).
The General Framework on Data Transfers Outside the EU

The legal framework for data transfers outside the EU is specified in the EU Data Protection Directive (DPD). The DPD provides for a number of legal bases to provide for an adequate level of protection in the EU. These include:

- Binding Corporate Rules (BCR), internal policies described by one or a multinational data controller to the Commission. Notably, the Commission does not consider corporate privacy standards in the U.S. to be equivalent. As a result, data transfers from the EU to the U.S. fall under the DPD's general prohibition. Standard Contractual Clauses (SCC), which also involve personal data, are U.S. companies that will rely on the BCR framework to ensure an equivalent protection.

The safe harbor declared the Safe Harbor Decision null and void on 8 Nov. 2015. The court held that European citizens' privacy would be undermined by mass surveillance in the U.S. and that Safe Harbor would not provide for effective judicial review by U.S. courts.

This is not necessarily the case, because Safe Harbor has benefits that can be considered an adequate level of data protection. These include:

- BCR, under which companies could rely on alternative legal bases to provide for an adequate level of data protection. This includes:
  - BCRs, which are contracts entered into by the Commission under which the data controller in the EU authorizes the company to transfer data within a corporate group.
  - SCCs, which are contracts entered into by the Commission under which the data controller in the EU authorizes the company to transfer data with entities in the U.S. that comply with EU data protection standards.

The above mechanisms have been widely criticized. Although the text has not been officially published, the upcoming Privacy Shield has already been widely criticized.

### BCR and SCC in the U.S.

Although the text has not been officially published, the upcoming Privacy Shield has already been widely criticized.

### Privacy Shield: New Rules and Unanswered Questions

After the expiration of the aforementioned grace period on 1 Oct. 2015, the EU Commission announced a new EU-U.S. data transfer agreement, the so-called Privacy Shield. To replace the Safe Harbor Agreement, the Privacy Shield aims to impose stronger obligations on companies based in the U.S. to protect the personal data of EU citizens. The new mechanism is meant to foster more comprehensive privacy and enforcement by the U.S. Department of Commerce (DoC) and the Federal Trade Commission (FTC). The following, points were announced for the Commission during its press conference:

- BCR and SCC on the Verge
- Although the text has not been officially published, the upcoming Privacy Shield has already been widely criticized.
New national possibilities will be established in one or more third countries of EU citizens' rights. U.S. companies using the Privacy Shield will be held with strict compliance to responding to complaints. The BCR and SCC will be expected to cooperate with EU DPAs.

In respect to complaints on possible access by national intelligence authorities on the U.S., a new Ombudsperson will be created to resolve disputes.

An annual joint meeting will be established, including EU DPAs, to oversee the implementation of the Privacy Shield arrangement.

However, this information was only provided orally during a Commission press conference. The text of the new agreement has not yet been published but is expected to be finalized by March 2016. The Commission has announced that it will make the text available in due course. The upcoming Privacy Shield has already been widely criticized.

Although the text has not been officially published, the upcoming Privacy Shield has already been widely criticized.

Most importantly, it has not been revealed whether adequate transfer mechanisms such as BCRs and SCCs can be used as a data controller, or whether one or both of these will need to be used in the manner as provided for in the U.S.

New complaints with EU data protection rules can lead to a prohibition on corporate data flows, then the outcome and success of these case will create a new paradigm. Furthermore, breaches can also lead to significant organizational risk for activities in Europe. The enforcement of the new Privacy Shield will ensure that cases are handled in a transparent and accessible manner under the General Data Protection Regulation (GDPR) which will enter into force in early 2018. The GDPR will impose fines up to 4 percent of a company’s worldwide group turnover. GDPR will also, in addition to the fines, impose a prospective ban on the transfer of personal data where there is a finding of insufficient protection in third countries, and in response to a new data breach or serious violation of the GDPR. This means that it is essential for companies to stay on top of the development of the new Privacy Shield.

WP 29 already announced that national regulators will be created to resolve disputes. This will be established, involving EU DPAs, to oversee the implementation of the Privacy Shield agreement.

Yet Another Grace Period

WP 29 already announced that national regulators will coordinate closely to assess the legal validity of Privacy Shield. In this regard, WP 29 deduced four criteria are the following:

- Adequate redress possibilities
- Adequate redress possibilities
- Adequate redress possibilities
- Adequate redress possibilities

Although the text has not been officially published, the upcoming Privacy Shield will initially be based on the basis of the new Privacy Shield agreement within the upcoming months, possibly in April 2016.

Although the text has not been officially published, the upcoming Privacy Shield will initially be based on the basis of the new Privacy Shield agreement within the upcoming months, possibly in April 2016.