The EU-US Privacy Shield

Update: the new transatlantic data transfer framework

By Michael Walther and Kai Gesing, LL.M.

Background

Since 1995 (or, more precisely, since EU member states implemented Data Protection Directive 95/46/EC), European data protection laws have enshrined the far-reaching principle that no personal data may be transferred to countries outside the European Economic Area (EEA) unless the destination country ensures an adequate level of data protection (and unless certain narrowly defined exceptions apply).

The Privacy Shield is designed to guarantee protection of Europe's fundamental rights.

© maxkabakov/iStock/Thinkstock/Getty Images

As this principle has been widely perceived as an obstacle to international trade and data flows, the European Commission has provided a set of instruments facilitating such transfers. These include Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) and – with respect to the United States – a Safe Harbor Framework (Safe Harbor). SCCs are model contracts for data transfers from data controllers within the EEA to service providers and other recipients established outside the EEA. BCRs are internal rules adopted by multinational groups of companies defining an internal policy for data transfers within the group. Safe Harbor permitted data transfers to companies in the United States that self-assess and self-certify their compliance with Safe Harbor and its data protection principles.

Following Edward Snowden's revelations in 2013 concerning US mass surveillance and intelligence activities, criticism of Safe Harbor increased significantly and included requests for its suspension by European data protection authorities (DPAs). The European Commission reacted later in 2013 by communicating 13 recommendations to improve the transatlantic framework and by entering into negotiations with the US government to address mass surveillance activities as well as a perceived lack of enforcement of Safe Harbor.

In October 2015, a decision reached by the European Court of Justice (ECJ) fueled these negotiations by invalidating the European Commission's July 26, 2000, adequacy decision that had implemented Safe Harbor. The ECJ emphasized privacy as a fundamental right in the European Union and particularly criticized that Safe Harbor only bound US companies and not US public authorities. As a result of the ECJ's decision, the protections in place with Safe Harbor were no longer available to serve as a basis for transferring personal data from the EU to the United States. This led to significant →

uncertainty for businesses on both sides of the Atlantic since European DPAs had only granted short transition periods and were not able to provide much guidance on what would serve as a safe basis for data transfers moving forward. Some DPAs even suggested applying the principles of the ECJ decision to other legal instruments as well – that is, to SCCs and BCRs. Others even questioned if an explicit consent obtained from the data subject would suffice for the transfer of personal data to the United States.

This vacuum was filled by the announcement in February 2016 of a new transatlantic data protection agreement, the EU-US Privacy Shield, which is not yet in effect as it requires an adequacy decision from the European Commission and this has yet to be made.

Elements of the Privacy Shield

The general goal of the EU-US Privacy Shield is to guarantee protection of Europe's fundamental rights to privacy during all data transfers and processing to and in the United States in compliance with European law and the requirements established by the ECJ, in particular those outlined in its 2015 Safe Harbor decision.

Participation in the EU-US Privacy Shield will remain entirely voluntary for US companies (as it was under Safe Harbor), however if a company elects to self-certify, it will be bound by the principles of the EU-US Privacy Shield. These principles mirror fundamental European data protection principles, including, for example, the individual's right to access his or her personal data with the right to request its correction, amendment and deletion; the right to obtain notice about data processing activities; and the purpose limitation principle. Onward data transfers made by a US data recipient are only permitted for specified, limited purposes in accordance with an individual's consent and solely on the basis of a contract with the third-party recipient ensuring its compliance with the principles of the EU-US Privacy Shield.

In comparison with the former Safe Harbor Framework, US companies certifying under the EU-US Privacy Shield will, however, face significantly stronger privacy obligations as well as an increased exposure to legal redress and remedies. Companies have to register with an alternative dispute resolution (ADR) provider and are under obligation to respond to privacy complaints made by EU individuals within a period of 45 days. The US Department of Commerce and the Federal Trade Commission will monitor self-certified companies and cooperate with European data protection authorities to address complaints. In addition, the United States enacted the Judicial Redress Act that provides EU nationals (once the EU is declared as a "covered country") with access to legal remedies in US courts.

Onward data transfers made by a US data recipient are only permitted for specified, limited purposes in accordance with an individual's consent.

With respect to intelligence activities, the US government has provided assurances (including from the Office of the Director of National Intelligence) that access to EU personal data by public authorities for national-security or law-enforcement purposes "will be subject to clear limitations, safeguards and oversight mechanisms" and restricted to specific purposes. This self-limitation by US national-security institutions is supplemented by the establishment of an ombudsperson to serve as a means for redress in the area of US intelligence activities.

Annual joint reviews of the Privacy Shield are intended to ensure the persistence of an adequate level of protection.

Criticism

Concerns have been expressed by various parties, including the Article 29 Working Party that represents European DPAs. In its opinion issued on April 13, 2016, the experts comprising the Working Party acknowledged the significant improvements in the proposed EU-US Privacy Shield compared with Safe Harbor. The regulators did, however, also express strong concerns and criticize a number of deficiencies in the proposed EU-US Privacy Shield – both in terms of commercial issues and with respect to access by public authorities. Its criticism concentrates inter alia on (a) alleged deficiencies in the implementation of the limitations to onward transfers and basic European data protection principles like the purpose limitation principle and the data retention principle, (b) deficiencies in the safeguards intended to ensure the exclusion of massive and indiscriminate surveillance of individuals, and (c) doubts about the efficiency of the intended redress mechanisms, especially with respect to the establishment of the ombudsperson for national signals intelligence activities. As a result, the →

Working Party requested further amendments to the EU-US Privacy Shield to remedy these concerns.

Status and next steps

While the Commission is expected to take the Working Party's opinion and recommendations into consideration when finalizing its adequacy decision, it seems unlikely the United States will provide additional assurances – in particular, with respect to national-security and enforcement activities. Likewise, it appears unlikely the Commission would deviate from its intended formal approval of the EU-US Privacy Shield, which is the final green light for data transfers to US companies self-certified within the new framework. The final adequacy decision was expected in June, but may be delayed, as the responsible Article 31 Committee consisting of member state representatives and chaired by the EU Commission recently concluded that they needed more time to consider the EU-US Privacy Shield.

Conclusions and outlook

- The EU-US Privacy Shield will essentially eliminate the legal uncertainty that currently exists and establish a framework for protecting EU personal data in the United States that is more robust than the previous instruments.

- A judicial review of the EU-US Privacy Shield is almost inevitable within the next two or three years and will likely be triggered by complaints made by EU individuals and national courts. The chances of success are hard to determine at this point, but data transfers made on the basis of and in compliance with the EU-US Privacy Shield would likely constitute one of the safest options moving forward.

- Alternative instruments (SCC and BCR) will possibly also face court challenges. With respect to the United States, these instruments may indirectly benefit from implementation of the EU-US Privacy Shield (for instance, enactment of the US Judicial Redress Act as well as limitations to US intelligence activities), and future decisions by the European courts concerning these instruments may provide an indication about the robustness of the EU-US Privacy Shield in terms of compliance with fundamental privacy rights in the EU.

- Companies in the United States are well advised to carefully analyze whether certification under the EU-US Privacy Shield and the related adjustment of existing processes are achievable – and desirable – due to the Privacy Shield's stricter requirements. As the new framework imposes detailed obligations on the certifying companies and requires coordination with third parties (for example, with respect to onward transfers to third parties and the registration of an ADR process), certification will likely require more time than was necessary within the previous framework.

- Companies in the EU that still transfer personal data (solely) based on the previous Safe Harbor framework are well advised to urgently discuss alternate legal instruments with their US counterparts or to seek alternative solutions for processing personal data from the EU. Companies that have already sought and implemented alternative solutions (for example, on the basis of the European Commission's SCCs) will likely experience less urgency in deciding whether and how to make use of the benefits offered by the EU-US Privacy Shield.

- For companies active in Germany, September 30, 2016, will be an important (but widely disregarded) deadline to bear in mind. After this date, companies may also face civil litigation under the German Injunction Act *(Unterlassungsklagegesetz)*, which was recently amended to improve enforcement of data protection provisions to the benefit of consumers. A grace period set forth in Section 17 of this bill, which concerns data transfers based on the previous Safe Harbor, will expire on September 30, 2016. ←

Michael Walther
Rechtsanwalt, Partner
Gibson, Dunn & Crutcher LLP
Munich

mwalther@gibsondunn.com

Kai Gesing, LL.M.
Rechtsanwalt, Of Counsel
Gibson, Dunn & Crutcher LLP
Munich

kgesing@gibsondunn.com

www.gibsondunn.com