Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 2 >>> FEBRUARY 2016

Privacy Shield

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 in line with the stringent requirements set out by the CJEU. 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 regulatory framework for data transfers outside the EU is stipulated in the EU Data Protection Directive (DPD). The DPD generally prohibits the transfer of personal data to countries that do not provide for an "adequate level of protection," though the question of adequacy is decided by way of a unilateral decision by the Commission. Notably, the Commission does not currently consider privacy standards in the U.S. to be adequate. As a result, a data transfer from the EU to the U.S. falls under the DPD's general prohibition. Nevertheless, in 2000 the European Commission decided that personal data sent to U.S. companies that self-certify under the Safe Harbor framework are considered to be adequately protected .

On 6 Oct. 2015, the CJEU declared the Safe Harbor Decision was invalid with immediate effect . The court held that EU citizens' rights to privacy would be undermined by mass surveillance in the U.S. and that Safe Harbor would not provide for effective judicial redress by EU citizens.

This is not necessarily the case, because beside Safe Harbor, companies could always rely on alternative legal bases to provide for an adequate level of data protection. These include:

- Binding Corporate Rules (BCR),[2] internal policies that have to be approved by national data protection authorities, to transfer data within a corporate group, or

- EU Standard Contractual Clauses (SCC)[3] , standard contracts issued by the Commission under which the data importer (i.e. the U.S. company) guarantees to comply with EU data protection standards and which contain information and liability obligations for the benefit of affected EU citizens.

Besides the aforementioned legal bases, the DPD only provides for very few exemptions from the restrictions on cross-border data flows (e.g. if the transfer is necessary for the conclusion or performance of a contract or for the defense in a legal trial). The data subjects' unambiguous and informed consent—which can be revoked at any time—may also constitute such a legal basis but only if given freely which is often problematic in the employment context. Hence, in light of these legal impediments, companies that rely on data transfers to the U.S. for day-to-day operations can, in the vast majority of cases, only rely on BCR (for intra-group data flows) or SCC.

[2] Cf. Communication on the Transfer of Personal Data from the EU to the U.S., dated 6 Nov. 2015, p. 4.

[3] Commission Decision 2001/497/EC, amended by Commission Decision C(2004) 5271, and Commission Decision C(2010)593.

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

BCR and SCC on the Verge

Shortly after invalidation of Safe Harbor, data transfers to the U.S. on the basis of BCR and SCC were called into question as well. This is because both tools, quite similar to the invalidated Safe Harbor, rely on the commitment of the data importer to adhere to EU data protection principles. Therefore, privacy proponents, including representatives from German Data Protection Authorities (DPAs),[4] argue that recent mass surveillance activities in the U.S., which were also challenged by the CJEU, would confirm that companies that are based in the U.S. are effectively unable to adhere to these standards.

The Article 29 Working Party (WP 29), an independent advisory body to the Commission consisting of representatives of all of the Member States as well as the EU Data Protection Supervisor, announced that it would assess whether the CJEU's reasoning from the Safe Harbor ruling could apply accordingly to alternative legal bases such as BCR or SCC. However, at the same time, WP 29 issued a grace period until the end of January 2016 to give the Commission and its U.S. counterparts time to negotiate a new framework that could replace Safe Harbor.[5]

Privacy Shield: New Rules and Unanswered Questions

After the expiration of the aforementioned grace period, the EU Commission announced on 2 Feb. 2016 a new EU-U.S. data transfer agreement, the so-called Privacy Shield, to replace the Safe Harbor Agreement.[6] To reflect the requirements set out by the CJEU, 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 oversight and enforcement by the U.S. Department of Commerce (DoC) and the Federal Trade Commission (FTC).[7]

The following points were announced by the Commission during a press conference:

- **National security and government access** to data will be subject to "clear limitations, safeguards and oversight mechanisms." According to Commissioner Jourová, "binding assurances" have reportedly been given by the U.S. to the EU regarding restrictions on U.S. mass surveillance.

[4] Cf. Position Paper of the DPA of Schleswig-Holstein.

[5] Statement of the Article 29 Working Party, 16 Oct. 2015, p. 4.

[6] European Commission, Press release, 2 Feb. 2016.

[7] U.S. Dep't of Commerce, Office of Public Affairs, Fact Sheet EU-U.S. Privacy Shield.

   ISSN 1473-3579

- New **redress possibilities** will be established to ensure effective protection of EU citizens' rights. U.S. companies using the Privacy Shield will be faced with deadlines for responding to complaints. The DoC and FTC will be expected to cooperate with EU DPAs.
- As regards complaints on possible access by national intelligence authorities in the U.S., a new **Ombudsperson** will be created to resolve disputes.
- An **annual joint review** will be established, involving EU DPAs, to monitor the implementations 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 it is expected to be finalized by March 2016. The Commission has announced that it will issue a new adequacy decision on the basis of the new Privacy Shield agreement within the coming months, possibly in April 2016.

Although the text has not been officially published, 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. Critics question whether the commitment to (restricted) access to information by public authorities will be binding for U.S. authorities and if so whether it will be enforced in practice. Furthermore, there is already a heated discussion as to whether the establishment of an ombudsperson will meet the CJEU's criterion of effective judicial redress. Many say that, in light of the CJEU's reasoning of the Safe Harbor judgment, it is just a matter of time until the new adequacy decision will be quashed by the CJEU upon the application of privacy activists or DPAs. It is therefore likely that the Privacy Shield will not bring much-needed comfort for companies that rely on data transfers to the U.S. BCR and SCC are therefore likely to remain the weapons of choice to transfer data safely to the EU.

Yet Another Grace Period

WP 29 already announced that national regulators will coordinate closely to assess the legal validity of Privacy Shield.[8] In this regard, WP 29 deduced four criteria from the CJEU's decision on the invalidation of Safe Harbor that are supposed to work as a benchmark for the new EU-U.S. agreement. The **four criteria** are the following:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated, balancing the rights of individuals and the needs of national security;
- An effective and impartial independent oversight mechanism should exist; and
- Effective remedies need to be available to the individual.

The impact of the EU-U.S. Privacy Shield on the use of BCR and SCC must still be assessed. In the meantime, WP 29 announced that DPAs would still accept these alternative transfer mechanisms until the assessment of the new Privacy Shield has been completed. This gives companies more time, but the legal uncertainty remains.

Conclusion

As of now, the legal situation for companies that rely on data transfers to the U.S. remains uncertain. It is unclear how the new Privacy Shield will turn out and whether this new deal will hold up to the scrutiny of DPAs and the CJEU. More importantly, it has not been resolved whether alternative transfer mechanisms such as BCRs and SCCs can be used in the future to transfer data to the U.S.

Non-compliance with EU data protection rules can lead to a prohibition on respective data flows, fines for the company and executives and in some cases even criminal penalties. Furthermore, breaches can also lead to significant reputational risk for activities in Europe. The situation will become even more acute with the introduction of the more stringent data protection framework under the General Data Protection Regulation (GDPR)[9] which will enter into force in early 2018. The GDPR will impose fines up to 4 percent of a company's world-wide group turnover or 20 million euros (approximately $22 million), whichever is higher. It is therefore essential for companies to stay on top of the developments in Europe to identify and implement a suitable solution.

In a worst case scenario, the new Privacy Shield will be shot down immediately and the BCR and SCC will no longer be permitted to be used. In this case, international players would be required to reconsider their data flows, for example by establishing processes and data centers that are solely based in the EU. In the meantime, companies with no proper foundation for their cross-border data flows face a serious risk of enforcement in the EU. Several DPAs have already made or announced requests for information to assess how international companies established with operations in Europe structure their data flows to the U.S. Enforcement actions are likely to follow.

[8] Cf. Press Release from 3 Feb. 2016.

[9] General Data Protection Regulation, draft version from Dec. 2015.