Bloomberg Law

Privacy and Security Law Report®

Data Transfers

EU-U.S. Privacy Shield Review—Not Bad but 'Room for Improvement'

EU-U.S. Privacy Shield

The European Commission's first annual review of the EU-U.S. Privacy Shield program for transferring EU citizen data to the U.S paints a fairly positive picture of the program, but the commission will remain focused on preventing the complacency that undid the predecessor Safe Harbor program, the authors write.

BY ROHAN MASSEY AND HEATHER SUSSMAN

On Oct. 18 the European Commission published its Report on the first annual review of the functioning of the EU-US Privacy Shield, confirming that overall the replacement for the Safe Harbour regime continues to ensure an adequate level of protection for the personal data transferred from the European Union to participating companies in the U.S., but that there is nevertheless ''room for improvement.'' According to the report, the U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield, such as new redress possibilities for EU individuals, and the certification process has been handled in an overall satisfactory manner. With the Commission saying that it ''stands strongly behind the Privacy Shield,'' the report makes a number of recommendations to the U.S. authorities to improve its implementation. In Justice Commissioner Věra Jourová's words, ''*The Privacy Shield is not a document lying in a drawer. It's a living arrangement that both the EU and U.S. must actively monitor to ensure we keep guard over our high data protection standards.*''

Rohan Massey is a partner at Ropes & Gray LLP in London and leads the firm's privacy and cybersecurity practice in Europe. Heather Sussman is a partner at Ropes & Gray LLP in Boston and is the co-head of the firm's privacy and cybersecurity practice

Background The Privacy Shield was formally adopted by the Commission on July 12, 2016 and U.S. companies were able to certify with the U.S. Department of Commerce (DoC) from Aug. 1, 2016. The Shield is designed to allow for and safeguard the transfer of personal data of EU individuals to the U.S. for commercial purposes. To reduce the risk of exposure to the sort of legal challenge that did for Safe Harbour regime, the Commission committed to review the functioning of the Privacy Shield on an annual basis. The first annual report sets out the Commission's findings and recommendations based on meetings held in Washington in September involving the EU's Civil Liberties, Justice and Home Affairs Committee (LIBE), the DoC, the Federal Trade Commission (FTC), and other U.S. authorities, as well as the Article 29 Working Party and representatives from U.S. industry.

The Good News Despite concerns raised by LIBE in September, the review confirms that the Privacy Shield continues to ensure an adequate level of protection for

the personal data transferred from the EU to participating companies in the U.S. The U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield, such as new redress possibilities for EU individuals. Complaint-handling and enforcement procedures have been set up, and cooperation with the European data protection authorities (DPAs) has been stepped up. For example, they have developed a standard referral form which facilitates the referral of a company to the DoC for further compliance review if a DPA believes that the company is not complying with the Privacy Shield. The certification process has also been fine-tuned and is functioning well with more than 2,500 companies certified so far. As regards access to personal data by U.S. public authorities for national security purposes, the Commission says ''*the relevant safeguards on the U.S. side remain in place*'' and the U.S. Department of State has taken measures to ensure that the Ombudsperson mechanism (the special instrument created by the Privacy Shield to address complaints concerning access to personal data by U.S. authorities for national security purposes), is fully functional and ready to receive and address complaints.

Room for Improvement As expected, the Commission nevertheless considers that the practical implementation of the Privacy Shield framework can be further improved in order to ensure that the guarantees and safeguards continue to function as intended. To this end, the Commission makes a number of recommendations:

- companies should not be allowed to publicly announce that they are Privacy Shield-certified until the DoC has finalised the certification;
- the DoC should conduct regular searches for companies falsely claiming participation in the Privacy Shield;
- the DoC should conduct compliance checks on a regular basis. Compliance checks could take the form of compliance review questionnaires sent to a representative sample of certified companies on a specific ''thematic'' issue (e.g. onward transfers, data retention), or the DoC could systematically request to be provided with the annual compliance reports of certified companies seeking to be re-certified;
- the DoC and European DPAs should work together to develop guidance on the legal interpretation of certain concepts in the Privacy Shield (e.g. with regard to the principle of accountability for onward transfers and the definition of human resources data); and
- the DoC and DPAs should strengthen their awareness raising efforts (e.g. to inform individuals about how to exercise their rights under the Privacy Shield).

National Security As regards national security, the Commission says it would be welcome if U.S. Congress would consider favourably enshrining in the Foreign Intelligence Surveillance Act (FISA) the protections for non-Americans offered by Presidential Policy Directive 28 (PPD-28). PPD-28 stipulates that U.S. surveillance activities must include appropriate safeguards for the personal information of all individuals, regardless of their nationality, or where they might reside. It also provides that such activities must always be as tailored and as targeted as feasible. FISA provides one of the main legal authorities on the basis of which U.S. public authorities can access the personal data of Europeans that has been transferred from the EU to Privacy Shield-certified companies in the U.S. Section 702 FISA authorises the acquisition of foreign intelligence information through the targeting of non-U.S. persons located outside the U.S. with the compelled assistance of U.S. electronic communication service providers. At the same time, it imposes a number of conditions and limitations aimed at ensuring targeted collection.

Finally, the Commission notes, separately in Q&As published alongside the report, that a number of Privacy Shield-certified companies have published transparency reports, which show (in bands of 500) the number of requests for disclosure of communications content a company has received during a given reporting period. For example, between January and June 2016, Facebook Inc. received between 500 and 999 requests for access to content under FISA, affecting between 13,000 and 13,499 user accounts, while Alphabet Inc.'s Google Inc. received between 500 and 999 such requests, affecting between 25,000 and 25,499 accounts. These figures, the Commission says illustrate that, as a percentage of total user accounts (for example, Facebook has two billion active accounts), the number of accounts affected by requests for government access to personal data ''remains limited.''

Comment It may be of little consolation in politically fraught times, but the Commission's annual report paints a fairly positive picture of the Privacy Shield, which some predicted might meet the same demise as its predecessor, the Safe Harbour. Indeed initial reports on the LIBE Committee's trip to Washington suggested that serious shortcomings were identified and unaddressed.

Civil Liberties Chair, Claude Moraes, spoke of ''deficiencies'' which needed to be ''*urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses.*'' The progress revealed by the first review therefore testifies to an appreciation on both sides of the pond that transatlantic data flows are of crucial economic significance.

The review nonetheless appears in the shadow of the latest reference to the Court of Justice of the European Union, from the Irish High Court in Schrems II on model privacy contractual clauses, that there may be insufficient safeguards in U.S. law in relation to the processing of the personal data of EU citizens for national security purposes. The Commission will therefore remain focused on preventing the complacency that beset and ultimately undid the Safe Harbour from afflicting the Privacy Shield.

BY ROHAN MASSEY & HEATHER SUSSMAN

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

  PVLR ISSN 1538-3423