Bloomberg BNA
Privacy Law Watch™

January 22, 2018

Data Transfers

- EU Privacy Regulator Group's First Annual Privacy Shield Report—Ensuring a Future for the EU-U.S. Data Transfer Regime
  Privacy Shield

  Despite concerns expressed about the EU-U.S. Privacy Shield by EU lawmakers during its first annual review, the European Commission's report was arguably more positive than expected, and EU privacy regulators recognized the significant progress made in implementing the Privacy Shield, so there remains reason for optimism about the data transfer mechanism's long-term prospects, the author writes.

By Kevin J. Angle

Kevin Angle is counsel in the privacy & cybersecurity group at Ropes & Gray LLP in Boston.

By Kevin J. Angle

One of the key outcomes of the plenary meeting of the Article 29 Working Party (WP29) at the end of November 2017 was the adoption of its First Annual Report on the Privacy Shield following the joint review between European and U.S. authorities that took place in Washington in September 2017. Like the European Commission's report on the first annual review, which was published separately on Oct. 18, 2017, the WP29's report recognizes the progress made by Privacy Shield in comparison to the invalidated U.S.-EU Safe Harbour program. It nevertheless also identifies a number of “significant concerns,” some of which it suggests need to be resolved by the Commission and U.S. authorities before the General Data Protection Regulation (GDPR) takes effect on May 25, 2018. These include the appointment of an independent Ombudsperson as well as further guidance and transparency on the rules of procedure. Should these, and other concerns which the WP29 says should be addressed by the second joint review at the latest, not be remedied within the given timeframes, the WP29 threatens “appropriate action, bringing the Privacy Shield Adequacy decision to national courts for them to make a reference to the [Court of Justice for the European Union] for a preliminary ruling.”

Background

The Privacy Shield was formally adopted by the European 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. Currently, over 2,600 organizations are self-certified under Privacy Shield to facilitate such transfers.

In order to reduce the risk of exposure to the sort of legal challenge that invalidated the Safe Harbour regime, the Commission committed to review the functioning of the Privacy Shield on an annual basis. The Commission held its first joint review with U.S. authorities on September 18 and 19, 2017 in Washington and published its report on the review a month later. The report finds that U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield but also makes recommendations to improve the functioning of the Shield. In addition to the Commission, representatives of the WP29 participated in the Joint Review, along with the EU's Civil Liberties, Justice and Home Affairs Committee (LIBE), the DoC, the Federal Trade Commission (FTC) and other U.S. authorities, and representatives from U.S. industry. The WP29 set out its own findings and assessments—some of which are echoed by the Commission—in its First Annual report on the Privacy Shield.

The Commercial Aspects of the Privacy Shield

The WP29 starts on a positive note by welcoming the efforts made by U.S. authorities to set up a comprehensive procedural framework to support the operation of the Privacy Shield through, for example, the strengthening of the checks performed prior to the listing of certified organizations. However, it identifies a number of important issues that it considers unresolved.

Privacy Shield Principles

In relation to the Privacy Shield principles, the WP29 says that more precise guidance should be provided with respect to the application of the Choice Principle on when and how an individual can opt out from the processing of his/her data for a new purpose, and with respect to the application of the Notice Principle, including the timing for certified organizations to give notice to individuals. The WP29 also notes that while DoC had set up reminders regarding companies' accountability for onward transfers, no general guidance was provided on the topic and the content of updated contract clauses on onward transfers was not checked by the U.S. authorities.

The WP29 additionally calls for increased oversight and supervision of compliance with the Privacy Shield Principles through ex-officio investigations and continuous monitoring of certified companies. It observes that monitoring of compliance with the Principles by the U.S. authorities seems strongly focused on the certification and recertification process. After completion of the (re)certification procedure and in particular where no concrete suspicion of a breach has arisen, however, there appears to the WP29 to be a lack of oversight by the U.S. authorities. The WP29 noted the importance of such oversight in light of the Schrems decision's emphasis on effective detection and supervision.

Data Processors

The WP29 also asks the U.S. authorities to distinguish more clearly the status of data processors from that of data controllers both at the time of their self-certification and at the time of further checks. In particular, the WP29 observes that several of the obligations included in the Principles are not suitable for data processors, as it is always the data controller that determines the purposes and means of the

processing of the data. The WP29 notes, for example, that in order to respect the principle of purpose limitation, U.S. organizations receiving data for processing purposes should not be able to decide to process the data for their own, separate purposes.

Handling of HR Data

One potential conflict with the interpretation of U.S. authorities noted by the WP29 pertains to the handling of HR data. According to the WP29, the DoC's position is that, like in the Safe Harbour, only the processing of data of employees within the same company falls within the category of human resources data under the Privacy Shield. As a result, employee data transferred to a processor within the U.S. would not benefit from additional safeguards for HR data, notably the extended supervisory powers for the panel of EU data protection authorities (DPAs). In the WP29's view, however, any data concerning an employee in the context of an employer-employee relationship from an EU company may only be transferred lawfully under the Privacy Shield if the receiving company has an active HR data certification. The WP29, therefore, calls on the European Commission to address the issue and, if necessary, engage in negotiations with the U.S. authorities in order to amend the Privacy Shield mechanism accordingly.

Automated-Decision Making/Profiling

Similarly, the WP29 would like to see further improvements with regard to the rules governing automated-decision making/profiling. The WP29 has previously “deplored” the lack of guarantees in the Privacy Shield regarding automated decisions, which produce legal effects or significantly affect the individual. Following the joint review, however, the indications are that none of the data transferred under the Privacy Shield are processed through automated decision making systems, and that specific rules exist under US law in certain fields. In its October 18, 2017 report, the Commission called for further study of the issue. Nonetheless, the WP29 requests that the Commission contemplate providing for specific rules concerning automated decision making to provide additional safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, as under GDPR.

The Self-Certification Process

The WP29 has also identified what it considers problems with the self-certification process for companies which it says should be enhanced to ensure uninterrupted protection for data subjects and rapid compliance with the Privacy Shield principles. It refers in particular to the fact that a certification can remain active on the DoC list for as much as 30 days after expiration, potentially resulting in gap in the protection of data received from the EU by the U.S. company during this period.

Remaining Issues

Finally, the WP29 refers to outstanding issues from the adequacy decision that it had previously raised in its earlier Opinion 01/2016., These include what the WP29 characterizes as the absence or the limitation to the rights of the data subjects such as the right to object and the right to access, the absence of key definitions in the Privacy Shield, and the “overly broad exemption” for publicly available information.

Access by Public Authorities to Data Transferred to the U.S.

Again beginning on a positive note, the WP29 welcomes the efforts made by the U.S. government and legislator to become more transparent on the use of their surveillance powers. As with the commercial aspects of Privacy Shield, however, the WP29 finds that significant points of concern remain unresolved.

FISA and the Executive Order

Most specifically, the collection and access of personal data for national security purposes under both section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 still remains an important issue for the WP29. The WP29 wants to see further evidence or legally binding

commitments to substantiate the assertions by the U.S. authorities that the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis.

With, at the time of writing, a decision on whether and how to re-authorize section 702 FISA imminent, the WP29 would like to see several changes introduced. These include providing for precise targeting, along with the use of the criteria such as that of "reasonable suspicion," to determine whether an individual or a group should be a target of surveillance, subject to stricter scrutiny of individual targets by an independent authority ex-ante. The U.S. House of Representatives version of the re-authorization, passed on Jan. 11, would leave section 702 FISA in place in its current form through 2023. The bill still requires Senate approval.

The WP29 is concerned about the uncertainty and unforseeability of how EO12333 will be used for the collection of data for national security purposes. As it did in its earlier opinion the WP29 underlines that "it should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place," which means including as regards "data 'on its way' to that country." It identifies, as did the Commission in its report, the Presidential Policy Directive 28 (PPD-28) as important in this context as it provides for the only safeguards and limits to the collection and use of data collected outside the U.S. since the limitations of FISA or other more specific U.S. law do not apply. However, no new information was provided during the joint review in particular on the interpretation of PPD-28, especially on the express purposes allowing for the use of data, nor on additional elements as to the amount of personal data collected. The WP29 calls on the Privacy and Civil Liberties Oversight Board (PCLOB) to finish and issue its awaited report on EO12333 "to provide information on the concrete operation of this Executive Order and on its necessity and proportionality."

The WP29 also stresses that it sees the PCLOB as an independent body, to be an essential element of the oversight structure. It therefore identifies as a priority the need to appoint members to the vacancies on the PCLOB as soon as possible.

Redress for EU Individuals

Another significant issue for the WP29 is redress for EU individuals, specifically as identified in Schrems II, the availability of redress for EU citizens under the Administrative Procedure Act (APA) as well as under FISA. The principal problem, the WP29 says, appears to concern the "standing" requirement applicable to surveillance cases in US federal courts. The U.S. Supreme Court held in Clapper v Amnesty Int'l, 568 U.S. 398 (2013) that "standing" in federal courts requires "that plaintiffs have sustained or will sustain direct injury or harm and that this harm is redressable." The WP29 says that, under the procedural requirements as currently interpreted, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing an action against a surveillance measure on the basis of section 702 FISA or EO 12333. The WP29 will therefore "continue to follow closely the evolution of these cases as they could provide additional guarantees concerning the effectiveness of judicial redress offered before U.S. courts." In the meantime, the WP29 remains concerned that redress by EU citizens before US courts is still to be effectively guaranteed due to the problematic admissibility threshold of the "standing requirement."

The WP29 refers to the Ombudsperson as "a key element" designed to compensate the lack of or uncertainty over effective redress before the courts. The Ombudsperson should therefore be appointed as soon as possible, the WP29 says, and the exact powers of the Ombudsperson mechanism need to be clarified through the declassification of internal procedures concerning the interactions between the Ombudsperson and the other oversight bodies. Based on current information, the WP29's view is that the powers of the Ombudsperson to remedy non-compliance vis-à-vis the intelligence authorities are not

sufficient in the light of Article 47 EU Charter of Fundamental Rights. The Ombudsperson should also be able to bring the matter before a court.

Comment

Following the joint review meeting in Washington, and despite concerns expressed at the time by LIBE representatives over “deficiencies” which needed to be “urgently resolved to ensure that the Privacy Shield does not suffer from critical weaknesses,” the European Commission's report was arguably more positive than expected. The WP29's First Annual Report, therefore, represents a serious reality check made even more stark by the express threat to take court action seeking a reference to the CJEU if certain issues aren't addressed by May 2018.

Priorities for the WP29 include a functioning Ombudsperson mechanism, “declassification” of internal procedures, clearer foresight of the use of the Executive Order and safeguards in Policy Directive 28 and filling the vacant positions on the PCLOB, “an essential element in the oversight structure.” Even if these priorities are met in this timeframe—some relatively straightforward, others politically less so—the WP29 threatens to initiate the referral process if its further concerns are not addressed by the time the second annual review comes round.

In the light of the Irish Data Protection Commissioner's robust action in the Schrems cases, such threats, should be taken seriously. The WP29 does, however, recognize the significant progress made in implementing Privacy Shield, and along with the Commission's more positive assessment, there remains reason for optimism. The Privacy Shield continues to provide a legitimate route for personal data to flow, or in the cloud float, across the Atlantic.

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