Bloomberg BNA

Privacy and Security Law Report®

EU-U.S. Privacy Shield

The European Commission and the U.S. Department of Commerce-approved updated version of the EU-U.S. Privacy Shield was green lighted by a regulatory committee of EU countries July 8 and will be formally adopted and finalized the following week, the authors write as they discuss the outlines of the new data transfer pact.

EU-U.S. Privacy Shield 2.0 Signed, Sealed and Delivered

BY FRANÇOISE GILBERT & MARIE-JOSÉ VAN DER HEIJDEN

The European Commission and the U.S. Department of Commerce have agreed on a new draft of the Privacy Shield agreement (Shield v 2.0). The documents that form the Privacy Shield v 2.0 are an updated version of those that were published in late February 2016. After its publication, the initial draft of the Privacy Shield agreement was strongly criticized by the Article 29 Working Party, the European Data Protection Supervisor, and the European Parliament, preventing its ultimate adoption. *See, e.g.*, Greenberg Traurig Alert ''Thumbs Down to Draft EU-U.S. Privacy Shield,'' April 14, 2016.

Françoise Gilbert is a partner at Greenberg Traurig LLP in Palo Alto, Calif. She is the author and editor of the two-volume treatise Global Privacy and Security Law, which analyzes the data protection laws of 68 countries.

Marie-José van der Heijden is an associate at Greenberg Traurig LLP in Amsterdam.

The currently available unofficial version of the final Privacy Shield v 2.0 documents appears to be largely based on the February 2016 version. However, the documents do contain more provisions, clarify many issues, and introduce some additional requirements. The primary changes are found in the Draft Commission Implementing Decision Regarding the Adequacy of the Protection Provided by the European Union-U.S. Privacy Shield (the Decision).

Among other things, the Decision clarifies that the new Privacy Shield also applies to the transfer of personal data from Iceland, Liechtenstein and Norway, and not only from the EU Member States. It also clarifies that certified companies will be required to include a provision in onward transfer contracts obligating the recipient of personal data to notify the Privacy Shield-certified company if the recipient can no longer provide the same level of protection as required by the Privacy Shield Principles (Principles). Certified companies will also be required to include an express obligation in contracts to require the deletion or de-identification of personal data after they are no longer relevant for the identified purposes of processing or for compatible purposes, with the exception of processing for public interests. The Decision also clarifies that the Privacy Shield will be administered by the U.S. Department of Commerce, and will be enforced by the Federal Trade Commission and the Department of Transportation.

Scope of Application

Like the EU-U.S. Safe Harbor, its predecessor, the EU-U.S. Privacy Shield will be based on a system of self-certification by which U.S. organizations commit to

the Principles. The Principles will apply to both data controllers and data processors, but data processors must also be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles.

The updated Decision clarifies that the Principles will apply solely to the processing of personal data by a U.S. organization in so far as the processing by such organization does not fall within the scope of European Union legislation. It is worth noting that a U.S. company that processes personal data of residents of the European Union or European Economic Area (EEA), and whose activities fall within the scope of Article 3 the General Data Protection Regulation (GDPR) should not assume that its self-certification under the Privacy Shield will be sufficient to demonstrate its compliance with all provisions of the GDPR that apply to its operations.

Article 3 of the GDPR provides that the activities of a data controller that is not established in the European Union fall within the scope of application of the GDPR when these processing activities are related to (i) the offering of goods or services to Individuals in the EU irrespective of whether a payment is required; or (ii) the monitoring of the behaviors of individuals when that behavior takes place in the European Union.

Transition Period

The updated Decision also clarifies that while the general rule will be that the Principles apply to a U.S. business immediately upon filing of the self-certification documents with the U.S. Department of Commerce, there will be an exception for cases where an organization has a pre-existing relationship with third parties.

If an entity files its self-certification documents within two months from the day when the Privacy Shield becomes effective, it will be granted a nine-month grace period to bring its commercial relationships in conformity with the rules applicable under the Accountability for Onward Transfer Principle. During that transition period, the organization must allow data subjects to opt-out, and when personal data is transferred to a third party acting as an agent, it must ensure that the agent provides at least the same level of protection as required by the Principles.

Updated Analysis of the Privacy Principles

The updated Decision contains numerous clarifications of its prior analysis of the Privacy Principles that was included in the February 2016 version of the Privacy Shield documents.

Data Integrity and Purpose Limitation

The Data Integrity and Purpose Limitation Principle provides that personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. The Shield v 2.0 clarifies that organizations must ensure that personal data is reliable for its intended use, accurate, complete and current.

Choice

Under the Choice Principle, data subjects may opt-out if their personal data is to be disclosed to a third party or used for a materially different purpose. The updated Decision clarifies that where a new purpose is materially different, but still compatible with the original purpose, data subjects also have the right to opt-out or object. In addition, it clarifies that special rules will apply to the use of personal data for direct marketing purposes, to allow individuals to opt-out at any time.

Accountability for Onward Transfers

The Accountability Principle states that transfers of personal data will be possible only: (i) for limited and specified purposes; (ii) on the basis of a contract or similar arrangement within a corporate group; and (iii) if that contract provides the same level of protection as guaranteed by the Principles. The updated Decision clarifies that the obligation to provide the same level of protection as required by the Principles must apply to all parties involved in the processing of the data so transferred, irrespective of their location, when the original third party recipient itself transfers the data to another third party recipient, for example a subprocessor.

Access; Correction

The Access Principle grants data subjects the right to obtain confirmation from an organization whether that organization is processing personal data related to them, and to have the data communicated within reasonable time. The updated Decision clarifies that data subjects will also have the right to correct, amend, or delete personal data that is inaccurate or has been processed in violation of the Principles. This right can be exercised without justification, and only against a non-excessive fee.

The additional comments address the use of data to make automated decisions that affect an individual. Such an automated individual decision may significantly affect a person and is based on automated processing of personal data with a view to evaluate that specific person. The updated Decision points to the significant discrepancies between the U.S. and EU regimes in this respect. U.S. laws offer specific protection in certain areas such as when data is used for making decisions regarding employment offers, or in connection with credit or lending decisions. While acknowledging that the use of automated processing as a basis for making decisions and such evaluations that relate to different personal aspects as work performance, creditworthiness, reliability and conduct is increasing, the Decision indicates that the U.S. and EU now have agreed that a dialogue on profiling and automated decisions and evaluations will take place during the annual reviews of the implementation of the Privacy Shield agreement. This future dialogue should resolve the issue posed by Article 15 of Directive 95/46/EC and Article 19 of Regulation (EC) No. 45/2001. These provisions lay down the right for individuals to object to such decisions that are based solely on automated means about them, unless certain conditions are fulfilled or appropriate safeguards are in place.

  PVLR ISSN 1538-3423

The updated Decision clarifies that the Principles will apply solely to the processing of personal data by a U.S. organization in so far as the processing by such organization does not fall within the scope of European Union legislation.

Recourse, Enforcement and Liability

The Recourse, Enforcement and Liability Principle requires organizations to provide robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data has been processed in a non-compliant manner, and includes effective remedies.

The additional comments provided in the updated Decision focus on enforcement. It is expected that organizations that have failed to deal appropriately with complaints will be subject to the investigatory and enforcement powers of the Federal Trade Commission, the Department of Transportation or another U.S. authorized statutory body that must effectively ensure compliance with the Principles. The updated Decision contains a lengthy analysis of the Recourse, Enforcement and Liability Principle that details the eight levels of redress—which must be addressed in a specific sequence—of the escalation procedure that will be available to EU residents who would have complained about the handling of their data, and would not have obtained resolution to their satisfaction.

Increased Focus on Transparency and Oversight

A significant portion of the analysis laid out in the Decision focuses on oversight and enforcement mechanisms, to address complaints and concerns that the United States did not aggressively enforce compliance with the Safe Harbor Principles. In its supplementary analysis, the Decision observes that the Shield provides for oversight and enforcement mechanisms in order to verify and ensure that U.S. self-certified organizations comply with the Principles, and that any failure to comply is adequately addressed.

Among the new measures introduced by the Privacy Shield, the U.S. Department of Commerce is tasked with monitoring whether the organizations listed on the Privacy Shield list as having self-certified are current in their obligations, and, if they are not, ensuring that they have returned or deleted the personal data that they received under the Privacy Shield. The Department of Commerce is also tasked with monitoring any false claims of participation in the Privacy Shield, and improper use of the Privacy Shield certification mark.

The Decision also clarifies that, on an on-going basis, the Department of Commerce will conduct ex officio compliance reviews of self-certified organizations. Those compliance reviews will include detailed questionnaires and investigations when it has received a specific complaint, when an organization does not provide satisfactory responses to its inquiries or where there is credible evidence suggesting a failure to comply with the Principles.

Access by U.S. Public Authorities

One of the key points of friction between the U.S. and the EU has been the nature and scope of the U.S. laws that regulate access that U.S. public authorities have to personal data of EU citizens stored on servers within the jurisdiction of U.S. public authorities.

After the opinion delivered by the Article 29 Working Party earlier this year, the European Commission directly assured it would incorporate a number of recommendations by the data protection authorities.

The updated Decision supplements the pre-existing analysis of the applicable U.S. laws. It clarifies that the EU Commission has analyzed U.S. law and determined that it contains a number of limitations on the access to, and use of, personal data transferred to the United States for national security purposes, as well as sovereign and redress mechanisms that provide sufficient safeguards for those data to be effectively protected against unlawful interference and the risk of abuse. It concludes that in the Commission's opinion, the current U.S. laws satisfy the standard set by the European Court of Justice in the *Schrems* judgment, Case C-362/14, EU:C:2015:650. This key finding may prove very valuable, for example in the current controversy regarding the validity of Standard Contractual Clauses in new legal proceedings initiated by Max Schrems in Ireland, or in case the newly adopted Privacy Shield were challenged before court.

The draft of the Privacy Shield further states that ''bulk collection will only be authorised exceptionally where targeted collection is not feasible, and will be accompanied by additional safeguards to minimise the amount of data collected and subsequent access (which will have to be targeted and only be allowed for specific purposes).'' The definition of ''feasible'' is left to practice.

Next Steps

The Privacy Shield should provide legal certainty to corporations that transfer personal data from the EU/EEA to the U.S. Under current EU national data protection laws—and later under the General Data Protection Regulation—personal data can only be sent to the U.S., a non-EU country, if the U.S. guarantees EU residents a level of legal protection that is essentially equivalent to that they receive in the EU. As this is not the case, the Privacy Shield was needed. However, the agreement also needs an adequacy decision. An adequacy decision is a decision adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC which establishes that a third country ensures an adequate level of protec-

tion of personal data by reason of its domestic law or the international commitments it has entered into. Then, personal data can be transferred from the 27 Member States and the three EEA countries to the U.S., without additional safeguards (adequacy decisions were issued for several countries throughout the world, for example, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Uruguay, Israel, New Zealand and the transfer of Air Passenger Name Record (PNR) data to the U.S. Bureau of Customs and Border Protection).

Such adequacy decisions are adopted pursuant to the comitology procedure, which involves the following steps: (i) a proposal from the Commission, (ii) an opinion of the Article 29 Working Party, (iii) an opinion of the Article 31 Committee, and (iv) the adoption of the decision by the College of Commissioners. At all times, the European Parliament and the Council can request the Commission to maintain, amend or withdraw the adequacy decision if they view its act exceeds the implementing powers provided in the Directive.

After the opinion delivered by the Article 29 Working Party earlier this year, the Commission directly assured it would incorporate a number of recommendations by the data protection authorities. The proposal was sent both to the Article 31 Committee and to the European Parliament, but the latter cannot block it. The Article 31 Committee that consists of representatives of all 28 Member States and the Commission voted on the Privacy Shield early July 8. The Article 31 group had to vote in favor by a qualified majority of 16 EU Member States that represent at least 65 percent of the EU population. On Monday, the European Commissioner Jourová will inform the Civil Liberties, Justice and Home Affairs committee of the European Parliament on the state of play. It is expected Jourová and U.S. Secretary of Commerce Penny Pritzker will sign the framework agreement at the beginning of next week.

  PVLR ISSN 1538-3423