THE
NATIONAL LAW REVIEW

Safe Harbor Replacement EU-US Privacy Shield Approved

Tuesday, July 12, 2016

On July 8, 2016, the Article 31 Committee, comprised of representatives of the European Union (EU) member states, voted to approve a revised Privacy Shield framework that is intended to replace the Safe Harbor framework invalidated by the European Court of Justice (ECJ) in October 2015 and provide another lawful method for U.S. companies to transfer the personal data of European citizens to the United States. Then, on July 12, 2016, the European Commission (EC) endorsed the Privacy Shield, establishing it as a valid alternative to the Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) in order to export personal data of EU citizens.

Article By Chanley T. Howell
Michael K. Chung James R. Kalyvas
Steven Millendorf Aaron K. Tantleff
Foley & Lardner LLP Legal News Alert

Communications, Media & Internet
Corporate & Business Organizations
Global
European Union

The Privacy Shield may still, however, be the target of scrutiny and legal challenges. A number of critics have already warned that the revised deal is "flawed" and toothless to prevent mass surveillance by the U.S. government once personal data is in the U.S. Additionally, four EU member states abstained: Austria, Bulgaria, Croatia, and Slovenia. Not surprisingly, Max Schrems, the Austrian law graduate and privacy advocate whose successful challenge to the Safe Harbor resulted in its invalidation last year, has already vowed to challenge the legality of the Privacy Shield.

Impact to Businesses

Any U.S. company that receives personal data from the EU must adopt one of the approved mechanisms for cross-border transfers of personal data: (1) Standard Contractual Clauses, (2) Binding Corporate Rules (for inter-company/affiliate transfers), or (3) Privacy Shield. Similarly, companies in the EU that transfer personal data from the EU to the U.S. must ensure that one of the approved mechanisms is used to validate such transfers to companies in the U.S. Since any company seeking to export personal data from within the European Economic Area must do so in compliance with a valid legal mechanism, companies should now (1) determine whether self-certifying to the Privacy Shield makes sense for their organization and (2) if so, conduct a gap analysis between its current practices and the Privacy Shield requirements and remediate deficiencies to enable the company to self-certify to the Privacy Shield. If an organization decides not to utilize Privacy Shield, it must determine and implement an alternative mechanism of transfer in order to legally transfer personal data from the EU to the U.S., as any transfer not following one of the approved mechanisms would not be legal.

Background

The Safe Harbor agreement was relied on by approximately 4,000 U.S. companies to legally transfer the personal data of EU citizens to the United States. However, in October 2015, the Safe Harbor agreement was invalidated by the ECJ in the *Schrems* case on the grounds that the U.S. surveillance activities brought to light by Edward Snowden threatened the privacy rights of EU citizens without any means for judicial redress. The decision put at risk the transfer of personal data between the European Union and the United States. Since then, representatives of both the EU and the U.S. have been negotiating a new framework for cross-border data transfer that would comply with the laws and regulations governing the privacy rights of EU citizens.

In February 2016, the EC revealed the details on the proposed Privacy Shield framework designed to replace the

invalidated Safe Harbor agreement. The original draft of the Privacy Shield was met with concerns by EU regulatory organizations, and on April 13, the European Union's Article 29 Working Party (Article 29) issued an opinion rejecting the draft Privacy Shield because, among other reasons, it believed that the Privacy Shield did not preempt "massive and indiscriminate" bulk surveillance of EU citizens; it believed that there needed to be a built-in mechanism for adjusting the Privacy Shield for the upcoming General Data Protection Regulation (GDPR); and it was not convinced that the Ombudsman would have the necessary independence and authority to enforce the requirements of the Privacy Shield and address EU citizen complaints. On May 27, the European Parliament officially asked the EC to renegotiate with the United States to address the concerns in the Privacy Shield. The call to renegotiate created a significant amount of uncertainty for U.S. companies wishing to transfer and process data of EU citizens, with some rushing to try to quickly implement other approved mechanisms of transfer.

Since this time, U.S. officials and the EC have been meeting to address these concerns. On July 8, they unveiled the revised Privacy Shield concurrently with the announcement that the Article 31 Committee had reviewed and approved its adoption. The revision is accompanied with a Draft Commission Implementing Decision Regarding the Adequacy of the Protection Provided by the European Union-U.S. Privacy Shield (the Implementing Decision), which has now been adopted by the Commission.

Privacy Shield Requirements

The following is a summary of the key elements of the Privacy Shield:

- **Contract Requirements for Onward Transfers of Personal Data to Third Parties.** Companies that participate in the Privacy Shield must include a number of new provisions in their contracts with third parties (e.g., service providers, business partners, etc.) when personal data will be transferred to such third parties. These provisions include: (a) the third party must notify the company transferring the data if it can no longer provide the level of protection required by the Privacy Principles described in the Privacy Shield (the Principles); (b) personal data must be deleted or de-identified by the third party after the data is no longer needed for the identified processing purpose or compatible purposes; (c) service providers using personal data may only act on instructions from the "data controller" (e.g., the company transferring the personal data to the service provider) and assist the data controller in responding to individuals that exercise their privacy rights under the Principles. Thus, companies will need to consider what changes or amendments will need to be made to these types of agreements.

- **Individual's Rights to Modify Personal Data.** The Access and Correction Principle provides a data subject with the right to obtain confirmation whether the organization was processing personal data that related to the data subject and, if so, to get access to the data within a reasonable time. The Privacy Shield, as finalized, now clarifies that individuals will also have the right to correct, amend, or delete inaccurate personal data or personal data that has been processed in violation of the principles. Organizations may not charge an excessive fee for a data subject to exercise these rights and a data subject may exercise these rights without any justification.

- **Applicability to Downstream Processors.** The Accountability Principle under the original draft Privacy Shield required that transfers of personal data were only permitted for limited and specific purposes that were on the basis of a contract (or a similar arrangement within a corporate group) that provided for the same level of protection required by the Principles. The Privacy Shield now makes it clear that these requirements (and all of the Principles) must apply to all downstream parties that may be involved in the processing of data no matter where they are located.

- **Expanded Opt-Out Rights.** The Choice Principle in the original draft Privacy Shield provided an opt-out right for data subjects if their personal data was to be disclosed to a third party or to be used for a materially different purpose. As adopted, the Privacy Shield adds the additional requirement that when the new purpose is compatible with, but nonetheless materially different from, the original purpose, data subjects may opt out or object. Data subjects will now also be able to opt out at any time when personal data is used for direct marketing purposes.

- **Relevancy and Accuracy of Personal Data.** The Integrity and Purpose Limitation Principles described in the original draft of the Privacy Shield required that in order to collect and use personal data, the personal data must be relevant to the purpose of the processing. For example, if the personal data was collected to provide services to the individual, the data could not also be used for marketing purposes without the appropriate notice and consent of the individual. The Privacy Shield, as adopted, makes it clear that organizations must additionally ensure that personal data is reliable for its intended use and that it is accurate, complete, and current. Thus, companies will need to ensure that whatever personal data is collected is needed and relevant for the intended purpose for collecting the personal data, and that the data remains accurate.

- **Recourse Mechanisms for EU Citizen Redress.** The Implementing Decision details the manner of recourse that EU citizens will have for complaints that an organization has failed to comply with the Privacy Shield or failed to properly address such complaints. In particular, the Implementing Decision describes the eight levels of redress, each of which must be addressed in a specific sequence that will be available to EU citizens. These mechanisms of redress include a process for individuals to complain to companies, a requirement that companies respond to complaints within 45 days, and provide at no cost to EU citizens a means of Alternative Dispute Resolution (ADR) escalation if an individual is not satisfied with the company's response. In addition, EU Data Processing Authorities (DPAs) may refer complaints directly to the U.S. Department of Commerce (USDOC) or the U.S. Federal Trade Commission. Complaints regarding access by national intelligence may still be directly referred to the Ombudsperson as an ADR of last resort. Companies signing on to comply with the Privacy Shield will need to understand their obligations with respect to responding to and resolving privacy-related complaints from individuals.

- **USDOC Will Conduct Compliance Reviews.** To address Article 29's concern that the Safe Harbor framework was not well enforced, the Implementing Decision describes that the USDOC will be tasked with monitoring compliance of each organization that self-certifies to the Privacy Shield (including through official compliance reviews), and ensuring that violators will return or delete the personal data invalidly transferred under the guise of the Privacy Shield. Similarly, the USDOC is also required to monitor any false claims of participation or use of the Privacy Shield certification mark. Compliance reviews will include detailed questionnaires and investigations when the responses are unsatisfactory or there is a complaint. Thus, companies will need to have practices and policies in place to ensure it remains compliant with the Privacy Shield Principles.

- **Privacy Shield Extends Beyond EU Member States.** The Privacy Shield will apply not only to transfer of personal data from EU member states, but also to such transfers from Iceland, Liechtenstein, and Norway.

- **Restrictions on U.S. Government "Bulk Collection."** One important concern in Article 29's rejection of the initial draft of the Privacy Shield was around the U.S.'s indiscriminate bulk collection and access to personal data for national security surveillance activities. The revised Privacy Shield directly addresses this by stating that "bulk collection will only be authorized exceptionally where targeted collection is not feasible, and will be accompanied by additional safeguards to minimize the amount of data collected and subsequent access (which will have to be targeted and only be allowed for specific purposes)." The Privacy Shield does not define the term "feasible" and this is likely to be the subject of future litigation and regulatory enforcement actions. Nevertheless, the Implementing Decision describes in detail that the EC has analyzed U.S. laws and has recognized that such laws contain a number of limitations on the U.S. government's access to, and use of, personal data for national security purposes. It also describes that the redress mechanisms in the Privacy Shield, as finalized, provide sufficient safeguards for data subjects to protect against unlawful interference and the risks for abuse. The U.S. also provided written assurances that "the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms" while ruling out any indiscriminate mass surveillance of EU citizens. Notably, the Implementing Decision explicitly concludes that, in the Commission's opinion, the standards set by the ECJ in the *Schrems* decision are satisfied by the current U.S. laws.

- **Authority and Independence of Privacy Shield Ombudsman Established.** The Implementing Decision describes that it is satisfied that the role of the Privacy Shield Ombudsman will have not only the authority, but also the independence, to perform its roles under the Privacy Shield. The role of the Privacy Shield Ombudsperson will be comprised of a Senior Coordinator for International Information Technology and Diplomacy designated by the Secretary of State, as well as appropriate additional State Department officials necessary to assist in the performance of the Ombudsperson's duties. Additionally, the Privacy Shield Ombudsperson will work closely with other officials from other departments and will report directly to the Secretary of State and be independent from the intelligence community. The U.S. Secretary of State will be required to ensure that the Ombudsperson will carry out the function objectively and free from any improper influence that may have an effect on the Ombudsperson's obligations under the Privacy Shield.

- **Annual Review.** Data protection authorities from the EU and the USDOC will review the Privacy Shield framework on an annual basis to ensure it functions properly and adopt any changes to the Privacy Shield as required, such as due to new legislation. Companies that self-certify to the Privacy Shield will be required to adopt any implemented changes.

Future Discussions Regarding Principles and Requirements for Automated Decision Making

The Implementing Decision also noted that there is still a difference in the way the United States and the

European Union address companies' use of personal data to make automated decisions that affect individuals. The U.S. only provides regulation in certain sectors, such as employment offers and credit and lending decisions, while Europe and the GDPR provides broader protections across almost all sectors. The Implementing Decision describes that the U.S. and EU will discuss these issues during the annual reviews of the implementation of the Privacy Shield, which may include similar rights described in the GDPR, namely the right for an individual to object to such decisions that are based solely on such automated decision making, unless there are appropriate safeguards in place or there are other conditions that necessitate such decision making.

Recommendations

Determine Whether Privacy Shield is Right for You

The first step is to determine whether Privacy Shield is right for your organization. In addition to the Privacy Shield, other transfer options include the Standard Contractual Clauses and Binding Corporate Rules (for inter-company transfers). If your organization was previously Safe Harbor-certified, Privacy Shield may be a cost-efficient mechanism as you are probably already compliant to a degree with some of the requirements of the Privacy Shield. However, given the very likely legal challenges to Privacy Shield, consideration should be given to the relative cost of compliance and protections as compared to the other valid compliance mechanisms.

If you were not Safe Harbor-certified, the determination of whether Privacy Shield is appropriate for your organization requires consideration of the extent to which your company receives personal data from EU citizens, including the number of different organizations from which you receive personal data. If the amount of personal data transfers is limited, it may be more appropriate for the company to use the SCCs or BCRs. For those organizations that have already entered into the SCCs and BCRs and have undergone and implemented the additional measures required to comply, there is no need to certify to the Privacy Shield. However, if you have not already entered into the SCCs and BCRs, the cost to implement the SCCs and BCRs might be too high or might not effectively address your particular data transfer model, leaving implementation of the Privacy Shield as the only remaining option. Due to pending and likely future legal challenges, it still remains to be seen, however, whether the SCCs will remain a viable and legal alternative for cross-border data transfers. For the time being, they are. However, the pending challenge in the Ireland High Court in Dublin relating to a decision by the Data Protection Commissioner on EU-U.S. data transfer channels still remains. That challenge may wind its way all the way up to the ECJ to decide whether the SCCs that provide legitimacy to many existing trans-Atlantic data transfers are legal. The fate of the SCCs may rest upon that case.

Whether or not your organization was Safe Harbor-certified, companies with access to personal health care or financial data are more likely to have measures in place protecting personal data in a manner similar to the requirements of the Privacy Shield. Thus, certifying for the Privacy Shield should not be overly onerous.

While organizations certifying under the Privacy Shield will face increased scrutiny, the liability and risk to an organization for not having a legal mechanism for compliance is too great to be ignored. While there was once a time that a company could lay low, "allowing" some companies to avoid registering for Safe Harbor out of fear that by registering, they were adding their name to a public registry and opening themselves up to public scrutiny, the current global climate and lack of tolerance for not properly protecting personal data is so great that now every organization is subject to scrutiny, registered or not.

Finally, due to the anticipated legal challenges to the Privacy Shield, companies – particularly those "on the fence" about whether to self-certify to the Privacy Shield – may want to consider waiting until the dust settles a bit more on the future of and likelihood of continued validity of the Privacy Shield.

Privacy Shield Does Not Guarantee Compliance With the GDPR

Importantly, the updated draft of the Privacy Shield makes it clear that the Privacy Shield will only apply to processing by U.S. companies that do not fall within the scope of other EU legislation, and compliance with the Privacy Shield may not be sufficient for compliance with other EU legislation. In particular, organizations should not assume that compliance with the Privacy Shield is sufficient to satisfy the requirements of the activities described in Article 3 of the GDPR, which may apply to most organizations. Article 3 of GDPR brings organizations under the scope of the GDPR no matter where they are located when their processing activities are related to (1) the offering of goods or services to individuals in the EU regardless of whether any payment is required or (2) the monitoring of behaviors of individuals when that behavior takes place in the EU. In other words, most companies that may consider signing up for Privacy Shield will still need to comply with the GDPR when it becomes effective on May 25, 2018.

If Privacy Shield is Right for You, Conduct a Gap Analysis

If Privacy Shield is right for you, your business will need to conduct a gap analysis to determine what practices and procedures need to be put in place in order to submit the self-certification application to comply with the Privacy Shield Principles. This process involves an internal or external review process where the company's current practices with respect to collection, storage, processing, and security of personal data from the EU are evaluated against the Privacy Shield Principles. Prior to submitting the self-certification application, the organization will need to satisfy itself that it has appropriate policies and practices in place to certify to compliance with the Privacy Shield Principles. While many Privacy Shield requirements are common among U.S. companies (such as implementing reasonable security safeguards to protect personal data), many requirements are not. For example, as discussed more fully above, Privacy Shield requires downstream vendor contracts to require compliance relating to data minimization, data destruction, and access to personal data.

Effective Date

Registration via the USDOC website will open on August 1, 2016, allowing U.S. companies to register to be on the Privacy Shield list and self-certify that they meet the high data protection standards set out under the Privacy Shield. Registration will have to be renewed annually. While there is no transition period for the new Privacy Shield, the obligations described in the Principles of the Privacy Shield framework will apply upon certification, with a narrow grace period for complying with the new rules regarding onward transfers (allowing any organization that self-certifies within the two months after the effective date of Privacy Shield nine months to comply with the rules applicable under the Accountability for Onward Transfer Principle).

If Privacy Shield is Not Right for You, Implement Alternative Mechanisms as Applicable

If your company determines Privacy Shield is not warranted or desirable, then (assuming the company receives personal data from the EU) the company will need to adopt an alternative mechanism to comply with the EU data transfer laws such as the SCCs or BCRs. However, given the time and effort required to satisfy the requirements of the SCCs and BCRs, if your organization has not already gone down that path, it might be that you have little choice but to implement the Privacy Shield, as doing nothing is not an option and could result in a finding of non-compliance. Even though Safe Harbor was invalidated, the requirement to use a valid mechanism of transfer was not lifted. Thus, all organizations must consider one of the valid transfer mechanisms.

Looking Forward

For the first time since the invalidation of Safe Harbor, the uncertainty for U.S. companies regarding their obligations for protection and transfer of personal data of EU citizens is cleared. However, the clarity may be fleeting, given it is highly anticipated that the Privacy Shield will be challenged on multiple fronts. In addition to the challenges that await, there are other potential changes to the Privacy Shield in light of the UK voting to leave the rest of the EU. While the UK may have to adopt the EU data protections rules post-Brexit, it is unclear what that will look like.

While the Article 29 Working Party (made up of the national data protection authorities) previously stated that they would likely challenge the Privacy Shield in court without further clarification on the protection of EU personal data, in response to the revised Privacy Shield, they have indicated that they would meet on July 25, 2016, to review the Privacy Shield framework, as adopted, and issue a revised opinion.

You can find the final version of the Privacy Shield on the European Commission's website, along with its appendices, as adopted, and an FAQ.