DrinkerBiddle

Client Alert

July 15, 2016

EU-U.S. Privacy Shield Finally Approved – What's Next?

By Ken Dort and Jeremiah Posedel

The European Commission has finally approved, after four months of consideration, the so-called EU-U.S. Privacy Shield. The Privacy Shield replaces the invalidated Safe Harbor protocol as the new framework governing transfers of personal data to the U.S. from the EU. Accordingly, U.S. companies may begin to self-certify under the Privacy Shield commencing August 1, 2016. However, they should first carefully review the obligations imposed by the Privacy Shield and the consequences that self-certification may have on their businesses. In addition, they should assess the reliability of the new framework and prepare for significant resistance/push-back from some of the national Data Protection Authorities in the EU.

In this alert, we will explain what this final version of the Privacy Shield comprises and what steps should be taken by U.S. and EU businesses considering its use.

EU-U.S. Privacy Shield – Key Principles

As we have discussed in prior alerts, companies certifying under the Privacy Shield will have to commit to adhere to the following seven principles:

1. **Notice:** publishing privacy policies and links to Privacy Shield information;

2. **Choice:** providing consent and opt-out protocols to data subjects;

3. **Accountability for onward transfer:** concluding appropriate data transfer agreements with third-party recipients;

4. **Security:** implementing appropriate security measures;

5. **Data integrity and purpose limitation:** assuring that data is processed only for the purposes for which it has been collected;

6. **Access:** providing protocols enabling data subjects to confirm what processing is taking place, and to correct or delete information held about them; and

7. **Recourse, enforcement and liability:** implementing procedures to resolve complaints.

Criticism From the Article 29 Working Party (WP29) and Others

On April 13, 2016, the WP29 (a group comprising representatives of DPAs from each EU Member State) submitted to the European Commission an opinion assessing the Privacy Shield. In that opinion, the W29 acknowledged the improvements of the Privacy Shield over the Safe Harbor but nevertheless concluded that the Privacy Shield required more work to adequately protect the personal data of EU citizens. The WP29's issues focused on the following issues:

- U.S. authorities' apparent access to data transferred to the U.S. under the Privacy Shield;
- The proposed U.S. Ombudsman was not deemed sufficiently independent nor provided with powers adequate to effectively exercise and enforce its safeguarding duties; and
- The redress mechanisms were deemed not user-friendly nor effective.

These concerns raised were likewise recognized by the European Parliament and the European Data Protection Supervisor. Consequently, the Article 31 Committee (composed of representatives of each Member State's government) postponed its vote to consider whether further amendment to the Privacy Shield was necessary. However, on July 8, 2016, it did approve the Privacy Shield, thereby leaving the way open for the European Commission's vote on adoption/approval on July 12.

Recognizing the above criticisms, the European Commission revised some parts of the Privacy Shield and renegotiated several components. The resulting "amended" Privacy Shield contains tighter rules on data retention, onward transfers and more safeguards on the access to personal data by U.S. law enforcement, and the position of U.S. Ombudsman was renegotiated to re-enforce its independence from U.S. intelligence agencies. In addition, the following key changes were made to the initial version of the Privacy Shield published last March:

- **Stricter rules for data processing:** the most important change—stricter rules have been put in place on several processing activities.

- **Limitations to supplemental processing:** the approved Privacy Shield provides for a stricter purpose limitation requiring businesses "*not to process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.*"

- **Clearer retention periods:** the limitation of data retention provisions have been made more explicit. Companies may retain personal data only for as long as this serves the purpose for which the data was initially collected.

- **More restrictive conditions for onward transfers of personal data:** the obligation to provide the "same level of protection" when passing data to third parties was clarified and now includes an obligation for the third party in question to inform the certified business when it is no longer able to ensure the necessary level of data protection. The certified company will then have to take appropriate measures in response, such as making sure that the third party ceases processing the data.

Will the Privacy Shield Withstand Legal Opposition?

It remains uncertain whether the Privacy Shield addresses the concerns raised by the most vocal critics of the initial version. Max Schrems has already stated that he will challenge the legality of the Privacy Shield. Also, WP29 has scheduled a conference on July 25, 2016, to review the final version and to assess whether it satisfies all its prior concerns.

What Should U.S. Businesses Do Now?

We recommend that U.S. and EU companies consider and implement the following points:

- For U.S. companies that relied on the Safe Harbor, they should decide whether to self-certify under the Privacy Shield. While companies that have already switched to the use of EU Standard Contractual Clauses (SCC, or "Model Clauses") have no immediate need to act, those who have waited for the Privacy Shield's implementation and not yet effected an alternative to the Safe Harbor will need to take action now.

- U.S. companies that receive personal data from EU businesses will have to review their data processing activities carefully before deciding whether to self-certify under the Privacy Shield. The seven privacy principles noted above will apply immediately upon certification. However, organizations that certify in the first two months following the effective date of the Privacy Shield will be given a nine-month grace period to bring existing third party contracts into conformity with the onward transfer principle.

- Thus, it is advisable for those considering self-certification to thoroughly review their privacy practices and policies, and to make sure they comply with the Privacy Shield. The U.S. Department of Commerce has published a guide on how to self-certify under the Privacy Shield. More information can be found at the DOC Privacy Shield page.

- The Privacy Shield does not affect the validity of SCCs – these will remain a valid alternative for transferring data to the U.S. (and elsewhere out of the EU). Thus, there is no need to use the Privacy Shield to protect data transfers made under SCCs. However, because the validity of SCCs is being challenged before the High Court in Ireland, with a possible referral to the CJEU, companies may have to resort to the Privacy Shield at some point if SCC-based data transfers to the U.S. are also invalidated.

- Finally, since doubts have been expressed about the legality of the Privacy Shield, and it will likely be tested in EU courts soon, it would be advisable to put (or keep) in place SCCs as a backup line of protection, at least for the foreseeable future (recognizing that SCC-based transfers are also under review).

By taking these multiple actions, it will be easier for an organization to withdraw from the Privacy Shield at some future point because if it wants to retain data received under the Privacy Shield, it will still need to provide adequate protection for that data by another authorized means (for example by using SCCs).

If you have any questions about this alert, please contact the author or your usual Drinker Biddle contact.

Information Privacy, Security and Governance Team

Primary Contacts

Kenneth K. Dort
Partner
Chicago
(312) 569-1458
Kenneth.Dort@dbr.com

Jeremiah Posedel
Associate
Chicago
(312) 569-1504
Jeremiah.Posedel@dbr.com