JANUARY 2017

COMMENTARY

A New Swiss-U.S. Privacy Shield Replaces the U.S.-Swiss Safe Harbor

The U.S. Department of Commerce and Swiss Federal Data Protection and Information Commissioner ("FDPIC") recently finalized a new Swiss–U.S. Privacy Shield Framework ("Swiss Privacy Shield") that will allow companies to transfer Swiss personal data to the United States in compliance with Swiss data protection requirements. The Swiss Privacy Shield will replace the U.S.–Swiss Safe Harbor Framework ("Swiss Safe Harbor") and will apply conditions similar to those the EU–U.S. Privacy Shield Framework ("EU–U.S. Privacy Shield") established last summer for cross-border transfers of EU personal data.

As a result, no longer can organizations transferring Swiss personal data to the United States rely on the Swiss Safe Harbor. Those organizations with current Swiss Safe Harbor registrations will need to certify under the new Swiss Privacy Shield or implement an alternative means of complying with Swiss data transfer restrictions. Organizations can self-certify to the U.S. Department of Commerce (via the Privacy Shield website) and publicly commit to comply with the Swiss Privacy Shield starting April 12, 2017. Now is the time for organizations considering self-certifying to the Swiss Privacy Shield to review the principles and commitments of the new pact.

The Swiss Privacy Shield's replacement of the Swiss Safe Harbor follows closely after the European Court of Justice ("ECJ") invalidated the U.S.–EU Safe Harbor program in its October 6, 2015, *Schrems* decision on the ground that the program failed to provide adequate levels of protection to personal data transferred from the European Union to the United States.[1] The invalidation of the U.S.–EU Safe Harbor quickly led EU and U.S. officials to negotiate the terms of the new EU–U.S. Privacy Shield released in July 2016 to replace the defunct U.S.–EU Safe Harbor with a more robust and comprehensive transatlantic data-transfer scheme.[2] Shortly after the EU–U.S. Privacy Shield was released, the FDPIC announced in August 2016 that the shortcomings identified in the *Schrems* decision also applied to the Swiss Safe Harbor, thereby prompting the Swiss and U.S. governments to also negotiate a more stringent data-transfer pact.[3]

The Swiss Privacy Shield adopts requirements that are almost identical to those incorporated in the EU–U.S. Privacy Shield. For example, the Swiss Privacy Shield requires participating companies to annually certify with the U.S. Department of Commerce and to voluntarily adhere to the seven Privacy Shield Principles and 16 sub-principles as set forth in the EU–U.S.

Privacy Shield ("Privacy Principles").[4] Participating organizations also must develop comprehensive privacy notices that publicly declare their compliance with the Privacy Shield Principles and explain their data collection practices. Similar to the EU–U.S. Privacy Shield, the Swiss Privacy Shield carves out specific obligations for the transfer of Swiss employee data to the United States. Organizations intending to receive human resources ("HR") data from Switzerland must develop an HR privacy policy that incorporates the Privacy Principles. Participating organizations must provide a copy to the U.S. Department of Commerce and must ensure that the HR privacy policy is available to affected employees.

The new regime also offers Swiss individuals multiple methods to voice their concerns and seek recourse regarding the processing of their personal data. As with the EU–U.S. Privacy Shield, participating companies must provide free and independent recourse mechanisms to Swiss individuals, and they are subject to enforcement by the U.S. Federal Trade Commission or the U.S. Department of Transportation, where Swiss individuals also can assert complaints. Moreover, the ombudsman established under the EU–U.S. Privacy Shield also will be available to Swiss individuals concerned about the U.S. government's overreach or unlawful access to their personal data.

The Privacy Principles under the two frameworks mirror one another with a few limited exceptions. First, under both frameworks, participating organizations must enter into contracts with third-party recipients that require the same level of protection guaranteed by the Privacy Principles. Unlike the EU–U.S. Privacy Shield, however, the Swiss Privacy Shield does not offer participating organizations the same nine-month grace period to revise their third-party contracts in accordance with the Privacy Principles. Second, the FDPIC's authority substitutes for that of the EU data protection authorities' throughout the Swiss Privacy Shield. Third, the definition of "sensitive data" under the Choice Privacy Principle is modified slightly under the Swiss Privacy Shield to include "ideological or trade union related views or activities, or information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings."[5] Lastly, the U.S. Department of Commerce will work with the Swiss government at the first annual review to implement the binding arbitration option of the Swiss Privacy Shield.

Once the Swiss Privacy Shield is in effect, organizations can expect increased cooperation and oversight by both the U.S. and Swiss governments to ensure compliance with the new framework. Companies that voluntarily withdraw, fail to complete the annual recertification requirements, or are found to persistently fail to comply with the Privacy Principles will be published on the Privacy Shield website.

The FDPIC has stated that it will not undertake enforcement actions during the next three months while the Swiss Privacy Shield is underway. During this time, companies certified under the Swiss Safe Harbor will need to carefully review the new terms of the Swiss Privacy Shield as well as their own privacy policies in order to ensure that their privacy practices comply with the new framework, or alternatively, identify other legal methods to transfer Swiss personal data to the United States. Prior to self-certifying with the new Swiss Privacy Shield, organizations that participated in the Swiss Safe Harbor will also need to update their privacy policies to remove any references to the Swiss Safe Harbor, in addition to meeting the Swiss Privacy Shield's more stringent notice requirements. Once an organization has joined the Swiss Privacy Shield, it will be automatically withdrawn from the Swiss Safe Harbor, and the U.S. Department of Commerce's Privacy Shield team will revise its Swiss Safe Harbor record to reflect the date of certification to the Swiss Privacy Shield.

Those companies already certified to meet the more robust self-certification requirements of the EU–U.S. Privacy Shield will also need to certify compliance with the new Swiss Privacy Shield and should generally be able to do so with minimal effort. Starting April 12, 2017, organizations already self-certified to the EU–U.S. Privacy Shield can log into their Privacy Shield account, click on "Self-Certify," and select an option to add the Swiss Privacy Shield and other relevant information to their certification (for example, the organization's independent recourse mechanism). There also is a separate annual fee to the International Trade Administration[6] to join the Swiss Privacy Shield. Similar to the EU–U.S. Privacy Shield cost recovery program, the fee will be tiered based on the organization's annual revenue. Further information on the Swiss Privacy Shield's fee structure is expected to be provided on the Privacy Shield website soon. Additionally, organizations will be expected to recertify for both the EU–U.S. Privacy Shield and the Swiss Privacy Shield one

year from the date that the earlier of the two certifications was finalized. So for organizations that self-certified to the EU–U.S. Privacy Shield first, the recertification date for both the Swiss Privacy Shield and the EU–U.S. Privacy Shield will be one year from when the EU–U.S. Privacy Shield certification was finalized.

In short, companies considering the Swiss Privacy Shield must conduct the appropriate due diligence to ensure their data collection practices align with the Privacy Principles prior to certifying compliance. This means, among other things, carefully assessing existing privacy notices, offering Swiss individuals access and choice regarding the processing of their personal data, designating an independent dispute resolution body to resolve complaints, and implementing procedures for annually verifying compliance. This new framework will be reviewed annually by the Swiss and U.S. governments to assess whether it continues to provide an adequate level of protection to Swiss personal data. The U.S. Department of Commerce also announced its plan to make a Privacy Shield certification mark, and participating organizations will be informed when it is available for use. Participating organizations should, therefore, monitor the Swiss Privacy Shield for any other guidance or additional requirements.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Authors

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Jennifer C. Everett
Washington
+1.202.879.5494
jeverett@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Frances P. Forte
Atlanta
+1.404.581.8380
fforte@jonesday.com

Additional Contacts

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Giuseppe Mezzapesa
Milan
+39.02.7645.4001
gmezzapesa@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Chiara B.L. Formenti-Ujlaki, an associate in the New York Office, assisted in the preparation of this Commentary.

Endnotes

1 *See* Jones Day *Commentary*, "EU-U.S. Data Protection Safe Harbor: Not Safe Anymore."

2 *See* Jones Day *Commentary*, "The EU-U.S. Privacy Shield Approved."

3 The EU–U.S. Privacy Shield extends only to members of the European Economic Area ("EEA"). Because Switzerland is not a member of the EEA, transfers of Swiss personal data to the United States are not covered by the EU–U.S. Privacy Shield.

4 For more information on the Privacy Shield Principles, s*ee* Jones Day *White Paper*, "EU and U.S. Release Terms of Privacy Shield."

5 *See* Swiss–U.S. Privacy Shield Framework, Choice Principle.

6 The Privacy Shield program is administered by the International Trade Administration within the U.S. Department of Commerce.