European Union Implements New Privacy Shield

Effective as of July 12, 2016, the European Union has implemented the new US-EU Privacy Shield (the "Privacy Shield"). The Privacy Shield permits US organizations to self-certify that they meet the requirements for protecting Europeans' personal data ("EU Data"), allowing them to receive such data from EU organizations. The Privacy Shield is designed to replace the former US-EU Safe Harbor (the "Safe Harbor"), which was invalidated in a case decided by the Court of Justice of the European Union (the "CJEU") in October of last year.

The Privacy Shield builds upon the framework of the Safe Harbor and addresses several of the concerns raised by the CJEU. Most notably, the Privacy Shield incorporates several provisions that restrict the US government's ability to access, collect and use EU Data. There are, however, some broader changes that will affect other organizations.

Onward Transfer of Data

Under the Safe Harbor, the transfer of EU Data by an organization to a third party was governed by three principles: Onward Transfer, Notice and Choice. The Onward Transfer principle required that a third party adhere to the privacy protection required under the Safe Harbor, whether by certifying or entering an agreement to provide for such protection. The Notice and Choice principles required organizations to notify individuals that their data would be transferred to a third party and provide them with an opportunity to opt out of such transfer.

The Privacy Shield bolsters the Onward Transfer principle while retaining the Notice and Choice principles. Now, an organization may transmit EU Data to a third-party controller only if (i) such transfer is for a limited purpose that is consistent with the purpose for which such data was originally collected; (ii) such third-party controller enters into an agreement to provide the same level of protection as the Privacy Shield; and (iii) such agreement mandates that the third-party controller cease processing EU Data and remedy any situation in which it determines such third-party controller is unable to satisfy the requirements of the Privacy Shield.

In addition to these more stringent principles, the Privacy Shield also reverses the presumption of liability for third-party data processing. Previously, an organization that complied with the Safe Harbor was presumed not to be responsible for any third-party data processing that was inconsistent with the Safe Harbor. Now, the presumption is that the organization is responsible, even it if fully complies with the Privacy Shield.

Dispute Resolution

The Privacy Shield also overhauls the dispute resolution mechanisms that were available under the Safe Harbor. Whereas previously an organization simply needed to provide a readily available and affordable independent mechanism for asserting noncompliance, the Privacy Shield offers the following six methods for asserting noncompliance:

1. Contacting the organization;
2. Filing a complaint with an independent dispute resolution body (organizations are required to register with such a body);
3. Filing a complaint with a national Data Protection Authority ("DPA"), which will issue binding "advice" to resolve the issue;

PRACTICE LEADER
F. Paul Greene
fgreene@hselaw.com

PARTNERS
Kenneth W. Africano
kafricano@hselaw.com
Theresa A. Conroy
tconroy@hselaw.com
Brian M. Feldman
bfeldman@hselaw.com
Amy L. Hemenway
ahemenway@hselaw.com
John G. Horn
jhorn@hselaw.com
Thomas J. Hurley
thurley@hselaw.com
Edwin M. Larkin
elarkin@hselaw.com
Christopher M. Potash
cpotash@hselaw.com
Brian B. Shaw
bshaw@hselaw.com
Jeffrey A. Wadsworth
jwadsworth@hselaw.com
Richard T. Yarmel
ryarmel@hselaw.com

ASSOCIATES
Danial J. Altieri
daltieri@hselaw.com
John W. Brill (Jack)
jbrill@hselaw.com
Kyra Tichacek Keller
kkeller@hselaw.com
Benjamin E. Mudrick
bmudrick@hselaw.com
Michael Roche
mroche@hselaw.com
Edward H. Townsend (Ted)
etownsend@hselaw.com

4. Filing a complaint with a national DPA that is forwarded to the Department of Commerce for potential revocation of the organization's Privacy Shield certification;
5. Filing a complaint with the Federal Trade Commission; and
6. Filing for binding arbitration with the Privacy Shield Panel.

These six methods are in addition to any right to bring an action in court under the laws of the United States.

Reporting and Compliance

The Privacy Shield also increases the reporting and compliance obligations of organizations. Organizations must now retain records regarding the implementation of their privacy program and provide such records to regulators upon request. Additionally, organizations that leave the Privacy Shield must annually certify to the Department of Commerce that they are protecting any EU Data received in accordance with the Privacy Shield for as long as such data is retained.

Additional information about the Privacy Shield can be found at the Department of Commerce's Privacy Shield portal.

Click here to contact a member of HSE's Privacy and Data Security team, or contact one of the following HSE Privacy and Data Security lawyers for more information:

- F. Paul Greene 585-231-1435, fgreene@hselaw.com
- John G. Horn 716-844-3728, jhorn@hselaw.com

HSE Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS

ROCHESTER
1600 Bausch & Lomb Place
Rochester, NY 14604-2711
585.232.6500

BUFFALO
Twelve Fountain Plaza, Suite 400
Buffalo, NY 14202-2293
716.853.1616

ALBANY
111 Washington Ave., Suite 303
Albany, NY 12210-2209
518.434.4377

CORNING
8 Denison Parkway East, Suite 403
Corning, New York 14830-2638
607.936.1042

NEW YORK
733 Third Avenue
New York, New York 10017
646.790.5884