

Morgan Lewis

LAWFLASH

EUROPEAN COMMISSION RELEASES DETAILS OF NEW EU-US PRIVACY SHIELD

March 02, 2016

AUTHORS AND CONTACTS

Dr. Axel Spies, Gregory T. Parks, Mark L. Krotoski, Pulina Whitaker, Matthew Howse, W. Reece Hirsch

The new EU-US Privacy Shield seeks to address the European Court of Justice's criticisms in *Schrems* after the decision invalidated the Safe Harbor program for EU-US data transfers.

On February 29, the EU Commission released the Privacy Shield draft adequacy decision, four weeks after the initial announcement of the EU-US Privacy Shield, which has been put forth as the replacement for the invalidated Safe Harbor program that previously governed transfers of personal data between the European Union and the United States.[1]

As expected, the European Commission has attempted to tighten up the information governance obligations for US companies that import personal data from Europe following the European Court of Justice's criticisms of the now invalid Safe Harbor program in *Maximillian Schrems v. Data Protection Commissioner* in October 2015.[2]

This LawFlash provides an overview of the draft EU-US Privacy Shield and next steps for its adoption.

PRIVACY SHIELD LIST AND PRINCIPLES

- Similar to the Safe Harbor, the US Department of Commerce will maintain and make available to the public an authoritative list of US organizations (Privacy Shield List) that have self-certified to the department and declared their commitment to adhere to the Privacy Shield Principles.
- The EU-US Privacy Shield is premised upon the Privacy Shield Principles issued by the US Department of Commerce: notice, choice, accountability of onward transfers, data security, data integrity, purpose limitation, data access, recourse, enforcement, and liability. These principles are similar to the commitments of data importers under the Safe Harbor, but the necessary disclosures for each are much more detailed.
- US data importers must commit to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. In particular, they must
 - provide recourse for individuals who are the subjects of the data,

- ➤ implement follow-up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and
 - remedy problems arising from a failure to comply with the Privacy Shield Principles.
- A data importer commits to cooperate with the EU Data Protection Authorities (DPAs) by declaring in its Privacy Shield self-certification submission to the Department of Commerce that the organization adheres to the Privacy Shield Recourse, Enforcement and Liability Principles by committing to cooperate with the DPAs, including during investigations to resolve complaints. Specifically, a data importer must agree that it “will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.”

It is unclear at this time whether this commitment goes beyond the cooperation commitments that existed under the Safe Harbor.

- A data importer that self-certifies to join the Privacy Shield List to cover EU human resources data transferred in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data.
- While the Department of Commerce will publicly “name and shame” US companies that are not in compliance with the commitments under the EU-US Privacy Shield, the Federal Trade Commission (FTC) and other US agencies will likely enforce the obligations more vigorously than they did under Safe Harbor.

NEW AVENUES FOR LEGAL REDRESS

Data subjects will be able to lodge complaints under the EU-US Privacy Shield with the companies and with the relevant DPA:

With the company

- Complaints by the data subjects must be resolved by companies within 45 days.
- To resolve a dispute, a no-cost Alternative Dispute Resolution solution will be available.

With a DPA

- If the EU data subjects file a complaint with their national DPA, the DPA will then contact the FTC to ensure that unresolved complaints by EU citizens are investigated and resolved.
- As a last resort, there will be an arbitration mechanism to help ensure an enforceable remedy. Moreover, data importers must commit to comply with advice from European DPAs. This is obligatory for companies handling human resource data.

PRIVACY SHIELD OMBUDSPERSON CREATED FOR US STATE DEPARTMENT

A letter from US Secretary of State John Kerry describes the role of the new Privacy Shield Ombudsperson at the US State Department. The Privacy Shield Ombudsperson will work closely with “other United States

Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies.” It is intended that the ombudsperson will coordinate national security access to data transmitted from the European Union to the United States pursuant to the EU-US Privacy Shield, standard contractual clauses (SCCs), and binding corporate rules (BCRs).

NEXT STEPS

The adoption process will likely take several weeks, if not months, and the EU Parliament will play an active role in the process. Next steps will include the following:

- An EU committee composed of representatives of the EU Member States (the College) will be consulted.
- EU Data Protection Authorities (Article 29 Working Party) will give their opinion, before a final decision by the College.
- The EU Commission will vote on the “adequacy” of the EU-US Privacy Shield.

The European Commission has, in conjunction with US authorities, attempted to address the potential data privacy breach issues arising in the context of US authorities accessing European personal data. This issue was a key aspect of the *Schrems* decision, and is the most likely basis for any future challenge to the validity of the EU-US Privacy Shield. The next step will likely be an opinion from the Article 29 Working Party on the Privacy Shield Principles.

CONTACTS

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis lawyers:

Washington, D.C.

Axel Spies
Ronald W. Del Sesto

Silicon Valley

Mark L. Krotoski

San Francisco

W. Reece Hirsch

Philadelphia

Gregory T. Parks

London

Pulina Whitaker
Matthew Howse
Lee Harding

[1] See our February 2016 LawFlash “EU-US Privacy Shield to Replace Safe Harbor.”

[2] See our October 2015 LawFlash “EJC Rules EU-US Safe Harbor Programme Is Invalid.”

Copyright 2016 Morgan, Lewis & Bockius LLP | All rights reserved