Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

CALIFORNIA DELAWARE JAKARTA* NEW JERSEY NEW YORK PENNSYLVANIA WASHINGTON, D.C.

PRIVACY AND DATA SECURITY AND INTERNATIONAL ALERT

FEBRUARY 2016

"PRIVACY SHIELD" IS PROPOSED TO REPLACE INVALIDATED U.S. – EU SAFE HARBOR AGREEMENT AND KEEP DATA FROM EUROPE FLOWING

By Scott J. Wenner

The Safe Harbor agreement between the European Union and the United States permitted American businesses to import personal data of EU citizens based on self-certification of compliance with EU data protection laws. Safe Harbor was widely criticized in Europe as being too easily circumvented, too infrequently enforced and offering too little protection to the personal data of EU citizens.

Edward Snowden's 2013 claims that the U.S. National Security Agency was collecting vast quantities of personal data of foreign nationals provided to it by Internet companies dramatically escalated EU criticisms of Safe Harbor. Snowden's revelations led European data processing authorities ("DPAs") and EU representatives to insist on negotiations to strengthen Safe Harbor if termination of that agreement by the EU was to be avoided. While those negotiations slowly proceeded, the EU Court of Justice ("EUCJ") heard a claim by an Austrian activist, Max Schrems, alleging that Facebook - a Safe Harbor participant - violated the privacy rights of EU citizens by giving their personal data to the NSA. On October 6, 2015 the EUCJ concluded in its *Schrems* decision that the Safe Harbor agreement failed to protect Europeans from unlimited and indiscriminate collection, storage and review of their private information, and thus was invalid.

The EUCJ also declared that a national DPA is obliged to challenge decisions of the European Commission that approve agreements such as Safe Harbor, and now the Privacy Shield, when their investigations lead them to believe that an agreement with a non-EU country fails to protect privacy rights of their citizens. With that holding, the EUCJ's ruling removes the legal certainty that Commission approval of agreements negotiated with key trading partners can be relied upon before expensive practices and procedures are implemented to comply with their terms.

Response to Safe Harbor's Demise – The Privacy Shield

The *Schrems* decision caused great concern among the U.S. businesses that were relying on Safe Harbor for their flow of data from Europe, and created political pressure on the U.S. and EU agencies already negotiating revisions to that agreement. Moreover, the Article 29 Working Party ("Working Party")– an independent and enforcement-oriented advisory body on data protection comprised of representatives of the data protection regulators of all 28 of the member states – had adopted an aggressive posture on the effect of *Schrems* on the mission of national DPAs. The Working Party declared that the focus of the *Schrems* ruling on the purported overreach of the

NSA and complicit businesses, at the expense of privacy rights of Europeans, would prompt it to reassess the efficacy of *all* of the tools previously authorized for the transfer of personal data to the U.S. It ominously added that the DPAs within the EU were prepared to commence "coordinated enforcement actions" and any other "necessary and appropriate actions" if EU and U.S. negotiators failed to reach an appropriate accord by January 31, 2016.

On February 2, EU and U.S. negotiators announced that they had agreed on "a new framework for transatlantic data flows." Dubbed the "Privacy Shield," the agreement has not yet even been committed to paper, such was the urgency to announce a resolution. The information made available by the negotiators consists only of an outline of broad principles to which EU and Commerce Department officials agreed. According to a EU press release, the Privacy Shield will include:

- "Strong obligations" on U.S. companies on how personal data of Europeans is processed and privacy rights are guaranteed.
- "Robust enforcement," to include monitoring by the Commerce Department of the publication of privacy commitments to allow the FTC to enforce breaches as unfair trade practices.
- Undefined special treatment of human resources data from Europe, which obliquely will require employers to comply with decisions of European DPAs.
- Clear safeguards, limitations and oversight mechanisms applicable to access by public authorities to personal data transferred from Europe to the U.S.
- Effective protection of the privacy rights of EU citizens with eight channels for redress of their complaints and deadlines for their resolution, including free alternative dispute resolution and a referral mechanism from DPAs to the Department of Commerce and the FTC. Binding arbitration for injunctive relief will be available as a mechanism of last resort.
- An Ombudsman embedded within the U.S. State Department will be appointed to investigate claims of inappropriate monitoring by U.S. national security agencies.

The sketchy details provided have failed to relieve the uncertainty created by the *Schrems* decision, much less provide information necessary to begin planning. Given the vital connection the flow of data has to international trade, the lack of certainty is unsettling to business and regulators alike. Meanwhile, the Article 29 Working Party has declared that its approval will be necessary before the Privacy Shield can go forward, and it expects to be provided with the relevant documents by the end of February. It announced that its analysis would focus particularly on whether the Privacy Shield respects four essential guarantees: (i) clear, precise and accessible rules for processing personal data; (ii) an appropriate balance between national security objectives and privacy rights; (iii) an independent oversight mechanism to review the surveillance activity; and (iv) an effective remedy for excessive processing activity. The Working Party expressed its concern over satisfaction of the four guarantees, especially with respect to items (ii) and (iv) immediately above.

Next Steps as Confusion Reigns

After the requisite documents are presented to the Working Party, purportedly by the end of February, the Privacy Shield will have to be approved by the College of Commissioners, which consists of EU commissioners from all 28 member states. However, before this body decides the commissioners first must obtain the advice of the Article 29 Working Party. That step could prove to be an obstacle.

The head of the Working Party recently announced that the DPAs will not bring enforcement actions until March or April against companies that are reliant on the now-invalid Safe Harbor.

Tips for Navigating Through Uncertainty

Businesses continue to need to transfer and process data in today's global economy. As we wait for the details of the Privacy Shield to come together, here are some suggestions towards how to manage EU-U.S. data transfer:

- Art. 26 of the EU Directive provides several exceptions. Assess the nature and purpose of the data you seek to transfer with counsel to determine if any of the exceptions apply.
- Obtain consent for the data transfer. However, note that employee consent may not be considered "freely given."
- Consider implementing model contract clauses or binding corporate rules.
- Employ technology to cull and cleanse the data set so that records are not identifiable.
- Where possible, process the data in-country and seek to transfer a narrow, limited set of data. ◆

For more information about Schnader's International or Privacy and Data Security Practice Groups, or to speak with a member of the firm, please contact:

Scott J. Wenner
Co-chair, International Group
212-973-8115
swenner@schnader.com

Christian Moretti
Co-chair, International Group
212-973-8111
cmoretti@schnader.com

Anne E. Kane
Co-chair, Privacy and Data Security Practice Group
215-751-2397
akane@schnader.com

Stephenie Wingyuen Yeung
Co-chair, Privacy and Data Security Practice Group
215-751-2277
syeung@schnader.com

* *See: www.schnader.com/jakarta*