Client Update
EU-U.S. "Privacy Shield" Greeted Cautiously

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

WASHINGTON, D.C.
Jeffrey P. Cunard
jpcunard@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Michelle M. Hillenbrand
mmhillenbrand@debevoise.com

Tuesday's announcements of the European Commission and the U.S. Department of Commerce of a new "Privacy Shield" for the transfer of EU personal data to the United States have been followed yesterday by a reaction from the EU Article 29 Working Party that is decidedly cautious. What was announced on Tuesday are the broad outlines of the principles for the mechanism, not complete documentation. The Working Party, which comprises representatives of the EU data protection authorities ("DPAs"), the European Commission and the European Data Protection Supervisor, yesterday stated that it is withholding judgment, asking for the full text of the arrangement to be provided by the end of the month and, in the meantime, allowing companies to use other existing data transfer mechanisms.

WHAT IS THE PRIVACY SHIELD?

As compared to the Safe Harbor, which the European Court of Justice ("CJEU") struck down last October, the Privacy Shield would enhance companies' obligations to protect personal data of EU individuals transferred to the United States. It would require stronger monitoring and enforcement by the Department of Commerce and the U.S. Federal Trade Commission ("FTC"), including increased cooperation with the DPAs, and would provide multiple avenues for redress.

The announced elements of the Privacy Shield include:

- U.S. companies to which personal data is exported from Europe will be required to commit to robust obligations on the processing of that data and the protection of individual rights.
- Companies' commitments will be enforceable under U.S. law by the FTC. The Department of Commerce will monitor companies to ensure that they

publish their commitments. Companies will need to commit to complying with decisions of the DPAs.

- Critically, given that the Snowden revelations formed the backdrop to the CJEU decision, the U.S. government has provided written assurances to the European Commission that access to personal data by U.S. authorities for law enforcement and national security purposes will be subject to limitations, safeguards and oversight mechanisms. Access will generally be permitted only to the extent necessary and proportionate. Indiscriminate mass surveillance of EU personal data is to be prohibited.
- EU individuals will have several new redress possibilities:
  - EU individuals will be able to complain directly to U.S. companies about the handling of their data. U.S. companies will have to meet deadlines to reply to such complaints. Companies will need to commit to participate in arbitration, free of charge to EU individuals, regarding such disputes.
  - The DPAs will be able to refer complaints to the Department of Commerce and the FTC.
  - Complaints from DPAs about access by U.S. national intelligence authorities will be handled by a new ombudsperson within the U.S. Department of State.
- The Department of Commerce, the FTC and the DPAs will hold annual meetings to discuss the functioning of and compliance with the Privacy Shield.

WHAT ARE THE NEXT STEPS?

Following the advice of the Article 29 Working Party and consulting with a committee of EU Member State representatives, the European Commission will prepare a draft decision for adoption by the EU College of Commissioners (the Commission's political leaders) that, with the Privacy Shield, the United States provides adequate protection for EU-originating personal data. The U.S. side will make the necessary preparations to put in place the new framework, the monitoring mechanism and the ombudsperson. These steps are expected to take at least several weeks, with a projection of three months before the new arrangement is fully in place.

The February 3 press release from the Article 29 Working Party mentions its concerns with respect to the current U.S. legal framework, especially regarding the scope of government agencies' indiscriminate access to personal data and

legal remedies of individuals. It called on the EU Commission to communicate all documents pertaining to the new arrangement by the end of February.

Privacy advocates in Europe, including Max Schrems, the Austrian student who brought the case challenging the Safe Harbor that culminated in the CJEU judgment, have indicated that the Privacy Shield itself might be challenged, as a derogation of the rights of the DPAs.

WHAT SHOULD COMPANIES DO FOR NOW?

Other existing mechanisms for transatlantic data transfers, such as the EU Commission's Standard Contractual Clauses or Binding Corporate Rules, were not invalidated by the CJEU decision last fall and were not explicitly the subject of the EU-U.S. negotiations on the Privacy Shield. In its press release, the Article 29 Working Party stated that existing transfer mechanisms may still be used; however, in light of the CJEU judgment and continuing concerns regarding government access to data, such mechanisms will be scrutinized once the final arrangements for the Privacy Shield are known. Given the deadline at the end of February and the time required for the subsequent review, this situation is likely to continue for the near foreseeable future.

Whether companies that were Safe Harbor registrants will want to use the Privacy Shield when it becomes available is uncertain, at least until the details of the new arrangement are made known.

We will send a further note as soon as the final arrangements for the Privacy Shield are in place.

* * *

Please do not hesitate to contact us with any questions.