US-EU Announce Deal on Data Sharing "Privacy Shield" to Replace "Safe Harbor"

By Adrian P. Kendall, Esq. Three months after the European Court of Justice struck down the US-EU "Safe Harbor" agreement in the case *Maximilian Schrems v Data Protection Commissioner* (C-362- 14), the EU and the USA announced in early February that they have agreed to a successor data protection regime. In the words of the European Commission: "This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses." The new EU-US "Privacy Shield" will again allow companies to store Europeans' personal data on American computers, subject to adherence to more rigorous compliance requirements. Background: The European Court of Justice had invalidated the "Safe Harbor" regime in the *Schrems* case by finding that it gave personal data of EU citizens insufficient protection against American intelligence gathering activities. Although the negotiations were at times rocky and hard fought, the stakes were too high for the parties not to find common ground: failure to reach a deal could have (i) led to economically and politically damaging enforcement litigation by EU nation state data protection agencies to prevent the transmission of personal data outside of the EU, and (ii) severely hampered the efficiency and effectiveness of multinational commercial activities. "Privacy Shield" Summary: The new arrangement will impose increased obligations on companies in the U.S. to protect the personal data of Europeans and requires stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission, including through increased cooperation with European Data Protection Authorities (DPAs). "Privacy Shield" includes commitments by the U.S. that access by public authorities to personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, designed to prevent generalized access. Europeans will be able to raise any inquiry or complaint in this context with a dedicated new ombudsperson. "Privacy Shield" Key Elements: Business and industry representatives on both sides of the Atlantic have been asking for a clear and uniform interpretation of the *Schrems* ruling, as well as more clarity on the mechanisms they would be permitted to use to transfer data. The following elements of the "Privacy Shield" arrangement should provide a framework to address those concerns:

- Strong obligations on companies handling Europeans' personal data and robust enforcement: U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under U.S. law by the Federal Trade Commission. In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.
- Clear safeguards and transparency obligations on U.S. government access: For the first time, the US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and proportionate. The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement there will be an annual joint

review, which will also include the issue of national security access. The European Commission and the Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to participate.

- Effective protection of EU citizens' rights with several redress possibilities: Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies will have deadlines to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, alternative dispute resolution will be available free of charge. For complaints on possible access by national intelligence authorities, a new ombudsperson position will be created.

Next Steps: This agreement marks a political resolution; the full, intricate legal framework has yet to be hammered out, so affected companies should still be adhering to the interim guidance. The EU College of Commissioners has mandated that Vice-President Ansip and Commissioner Jourová prepare a draft "adequacy decision" in the coming weeks. In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and a new ombudsperson. Once the full framework is in place, affected US companies will need to gauge how they can effectively comply and at what cost as rigorous enforcement should be expected. Time will tell if the goals of data security, trust and economic certainty will be fully met, especially on the issue of limited access by the NSA and other intelligence gathering agencies. Opponents have already voiced concerns over how any US safeguard assurances can be believed in the wake of the Snowden revelations and other spying activities that have recently become public. Another legal challenge may well loom, but it is highly likely that the European Court of Justice will uphold the "Privacy Shield" data protection scheme in the absence of specific proof of a breach.