EU Court Strikes Down EU-US Privacy Safe Harbor: Implications for Smaller Businesses

Under European Union law, the collected personal data of EU residents can be transferred to other countries only if those countries provide adequate protection for the personal data. Since U.S. law is viewed by the EU as being inadequate, companies wishing to transfer personal data from the EU to the U.S. have had to take additional steps for the transfer to be legal under EU law. To simplify this process, the U.S. Department of Commerce negotiated a Safe Harbor program with EU authorities 15 years ago that enabled U.S. companies to register with the Department of Commerce and self-certify compliance. More than four thousand U.S. companies currently use the Safe Harbor program to permit them to transfer personal data from the EU to the U.S.

On Oct. 6, 2015, in a case called Schrems v. Data Protection Commissioner, the Court of Justice for the European Union (the EU’s Supreme Court) invalidated the Safe Harbor program. It is the equivalent of a U.S. Supreme Court ruling that a government program is unconstitutional. The precise legal holding in Schrems is that the Safe Harbor transfer program is invalid because it provides inadequate protection for the personal data of EU citizens transferred to the U.S. The CJEU found that the Snowden revelations showed that the privacy protections supposedly guaranteed by the Safe Harbor program could be overridden by U.S. national security demands.

The biggest legal change brought about by the decision is that national data protection authorities in individual countries now have the right and duty to police data transfers out of their respective countries, even if the recipient is enrolled in the Safe Harbor. Those transfers will have to meet the national privacy laws of the country in which they originate. If you were in the Safe Harbor, you have lost its legal protection and can get it back only through one of two other approaches the EU offers: using approved “contractual clauses” or adopting “binding corporate rules.” These approaches both have shortcomings and have not been popular with U.S. companies.
So what should you do? Your immediate first step should be to focus on the substance of your privacy policies and practices—what are you actually doing? If you are a smaller company that is not doing anything that would violate EU principles, then you are unlikely to be targeted by EU regulators and, even if targeted, you are unlikely to face major damages or fines. To develop a longer-term response, you will need to monitor developments. Watch the post-Schrems regulatory activities of the national data protection authorities as they begin to take shape. Also keep a close eye on the progress of the pending EU Privacy Regulation, which could make the issue moot. Finally, the U.S. Department of Commerce has promised to provide advice to companies about how to respond, and to try to negotiate an interim solution, though the feasibility of that effort is in doubt given the EU’s growing hostility to the Safe Harbor even before this decision.