CORPORATE COUNSEL
An ALM Website
corpcounsel.com | October 19, 2015

The Euro Court of Justice Safe Harbor Ruling Should Spur Careful Planning

From the Experts

Mary J. Hildebrand

Those alarm bells going off in the offices of in-house lawyers all over America on Oct. 6 had a distinctly continental ring. That's when the European Court of Justice (ECJ) invalidated the Safe Harbor data-sharing pact that allowed U.S. companies to transfer the personal data of E.U. citizens to the U.S. The ECJ decision, which went into effect upon issuance and cannot be appealed, has already injected additional uncertainty and disruption into E.U./U.S. business relationships on both sides of the Atlantic.

This is a political issue and even a cultural issue. But make no mistake—this is, first and foremost, a legal issue, and it demands prompt attention. If board members and senior executives haven't already come knocking on their in-house counsel's door demanding a clear action plan, they're probably on their way.

What's particularly challenging is how little uniformity exists across European data-privacy laws, even after this ruling. In fact, the ECJ specifically conferred on national data-protection authorities (DPAs) the right to independently investigate claims that the transfer of personal data from the E.U. to another jurisdiction does not comply with E.U. Privacy Directive 95/46/EC (Directive). The result? Each DPA could establish a separate standard for data transfer from its own country.

Bobby Hidy/Flickr

Abruptly removing Safe Harbor from the equation after 15 years means thousands of companies that routinely transfer personal data from the E.U. to the U.S. in reliance on that protocol must now change course. The E.U. Commission has approved a few alternatives (see below), although they are arguably not as business-friendly as Safe Harbor. Any analysis of alternatives to Safe Harbor should include the following steps:

1. Assess the impact of the ECJ decision on your business. It's important to consider all aspects of your operations—this decision applies not only to consumer-directed enterprises, but also to business-to-business operations, intra-company

transfers, payroll, and any other transactions that depend on the ability to move E.U. personal data to the U.S.

Since Safe Harbor was invalidated, it is as if it never existed. While some commentators fret that the DPAs may seek retroactive penalties, the more pressing issue may be personal data of E.U. citizens previously transferred and stored in the U.S. under Safe Harbor. While it's difficult to predict how the DPAs will proceed, the prudent course would be to develop a plan to transfer such data back to the E.U..

Counsel for financial institutions may be in a position to sit this one out. Safe Harbor never applied to financial institutions, and they should not be directly impacted by the ECJ decision.

2. Evaluate your alternatives. There are three primary alternatives for data-transfer in a post-Safe Harbor world. Fair warning: Each one has considerable downsides.

Consent: Individual E.U. citizens may consent to transfer of personal data to the U.S., provided that such consent is freely given, specific, informed and unambiguous. Assuming that sufficient information and choice is provided, such consent requires an affirmative act, or "opt-in," from the individuals.

Model Contracts: These are templates negotiated between the U.S. Department of Commerce and the European Commission that give American companies the right to legally transfer personal data from the E.U. to the U.S. They are often regarded as inflexible, since modifications are quite restricted. And, unlike Safe Harbor, the model contracts are governed by the laws of the E.U. member country where the individual citizen resides. As a result, a U.S. company that collects personal data across Europe may be compelled to have a separate model contract in each country.

Binding Corporate Rules: The E.U. Article 29 Working Party developed these rules to allow multinational corporations (or groups of companies) to make intra-organizational transfers of personal data across borders to the U.S. in compliance with E.U. data protection law. While binding corporate rules (BCRs) may provide companies with an opportunity to be creative on their own behalf, BCRs must also be approved by the DPAs in every E.U. country where the company operates, a process that can take months.

If you are required, as a condition of transferring data from the E.U. to the U.S. using these alternatives, to conform to the same rules that apply to a European citizen in the E.U., some interesting circumstances could arise. For example, this could leave U.S. companies in the same difficult position as under Safe Harbor if they receive a request, demand or subpoena from a U.S. government agency or intelligence service seeking the E.U. personal data. There's no doubt that this scenario is on the minds of E.U. regulators and, to the extent that the DPAs take early action, addressing this issue may be a priority.

3. Plan. U.S. companies that previously relied on Safe Harbor are now transferring data from the E.U. to the U.S. without any legal basis. Counsel for these organizations should take advantage of this period of uncertainty regarding enforcement in the E.U. to complete an internal assessment, evaluate the alternatives and develop an implementation plan. If the current flurry of emergency meetings and plenary hearings in the E.U. do not result in any new concrete alternatives, then U.S. companies should proceed to implement their plans.

There are legislative and diplomatic efforts under way that may impact this situation. The U.S. and the European Commission (E.C.) continue to negotiate a revised Safe Harbor, but it remains to be seen whether the ECJ decision will encourage a speedy conclusion or further complicate the process. In 2012, the E.C. introduced the General Data Protection Regulation (GDPR) to replace the Directive and standardize data privacy across the E.U.. If approved, the GDPR could become effective as early as 2018.

In the meantime, the only certainty we can expect is uncertainty. U.S. businesses have no choice but to develop and execute well thought-out plans grounded in the current reality. But they must also be prepared to quickly alter those plans in response to further, possibly sweeping changes in E.U. data protection laws.

Mary J. Hildebrand is the founder and chair of Lowenstein Sandler's privacy and information security practice and senior partner in the firm's tech group. She has more than 30 years of experience in strategic planning, commercialization, protection and management of intellectual property, technology and database assets around the world.