The EU/US Safe Harbor Is No Longer Safe, Says The EU's Highest Court. Is Your Data A Liability?

October 7, 2015

Today, Europe's top court, the European Court of Justice, ruled that a 15-year-old pact between the United States and the European Union which allowed American organizations to handle the personal data of Europeans (the EU/US Safe Harbor) was invalid. **The decision will have massive, far-reaching implications for American businesses and other organizations that are active in Europe.**

The Backdrop

Trans-Atlantic data transfers involving the personal information of Europeans must comply with the Data Protection Directive, which is a European pact that has been adopted by each member state (i.e., most of Europe, but not Switzerland). The Directive requires that a transfer of personal data to a non-EU country may take place only if that country ensures an adequate level of data protection and privacy. The Directive also provides that the EU Data Protection Commission may determine that a non-EU country ensures an adequate level of protection as a result of that country's own domestic privacy laws or an international treaty.

The Facts

The challenge to the Safe Harbor arose in legal proceedings between an Austrian citizen, Mr. Maximilian Schrems, and the Irish Data Protection Commissioner concerning the Commissioner's refusal to investigate a complaint made by Schrems. Schrems has been a Facebook user since 2008, and some or all of the data provided by Schrems to Facebook was transferred from Facebook's Irish subsidiary to servers located in the United States. Schrems lodged a complaint with the Irish Commissioner, alleging that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the US intelligence services (specifically the NSA), the law and practice of the United States do not offer sufficient protection against surveillance.

The Issues

In response to Schrems' allegations, Facebook pointed out that it was fully compliant with the EU/US Safe Harbor and the US Department of Commerce's requirements for participation in the Safe Harbor. The Irish Commissioner refused to consider the complaint because the EU Data Protection Commission had long ago ruled (in 2000) that the EU/US Safe Harbor was a valid basis for the trans-Atlantic transfer of personal data of European citizens. (As a technical legal matter, the case was a challenge of the validity of Commission Decision 2000/520/EC (26 July 2000) pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbor privacy principles and related FAQ issued by the US Department of Commerce.)

The Court's Conclusions

The Court concluded that the decision by the EU Data Protection Commission that the EU/US Safe Harbor is valid did not preclude a member nation's Data Protection Commissioner (in this case Ireland) from reaching the opposite conclusion. The Court ruled that the Irish Commissioner should have heard the complaint and made an independent determination whether the EU/US Safe Harbor provides adequate protection of the personal information of EU citizens in light of the fact that the US government's surveillance programs might not respect the privacy of EU citizens as interpreted under EU law.

The Court went further to evaluate the 2000 decision of the EU Data Protection Commission. It determined that in the US, national security, public interest, or law enforcement interests prevail over the Safe Harbor scheme, so that US organizations are required by US law to disregard the protective rules laid down by the Safe Harbor when they conflict with US policy interests. The Court then concluded that US law, and the Safe Harbor, enable interference by United States national security and law enforcement authorities with the fundamental rights of Europeans. This interference is incompatible with the Directive, said the Court.

Having reached these conclusions, the Court held that the Irish Commissioner was required to evaluate Schrems' complaint "with all due diligence" and following its "investigation," was obligated to "decide whether, pursuant to the Directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that country does not afford an adequate level of protection of personal data." The Court essentially remanded the case to the Irish Commissioner with instructions to evaluate the issues, and with the subtext that the EU/US Safe Harbor is inadequate.

You can read the Court's decision here, and the Court's press release here.

No appeal is possible, because the European Court of Justice is the equivalent of the U.S. Supreme Court—the court of last resort. Simultaneously, European leaders and US officials are negotiating a new agreement on trans-Atlantic data transfers. Today's decision will no doubt create a new degree of urgency in those talks.

What Does It Mean to Your Organization?

The likely outcome of this decision is that transfers of personal data made under the auspices of the Safe Harbor may violate European data protection laws. ***In other words the Safe Harbor is not really "safe" after all.*** Without the Safe Harbor, each country in the EU could reach different conclusions as to whether US privacy laws and practices satisfy the EU's Directive, which would require US companies to address each member nation's laws individually rather than satisfying a single set of EU requirements. This could create enormous obstacles to US organizations doing business in Europe.

As a result, organizations are well-advised to take a belt-and-suspenders approach (or "belt-and-braces" as they say across the Atlantic) by ensuring that data transfers are justified on another basis (in addition to compliance with the Safe Harbor). Those other bases include "binding corporate resolutions" (in which the organization essentially passes a binding corporate resolution and to comply with EU law with respect to EU personal data) and "model clauses" (which are contractual obligations to comply with EU privacy requirements). The binding corporate resolutions and model clauses have frequently been deemed more onerous for US organizations than the Safe Harbor's requirements, and have historically been less popular among US organizations.

--

© 2024 Ward and Smith, P.A.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.