WINSTON & STRAWN LLP

CLIENT ALERT

EU Court of Justice Kills Safe Harbor

7 OCTOBER 2015

The Snowden revelation that the United States conducted surveillance on citizens of other countries has had significant impact, including on the transfer of personal data from the EU to the US. The latest impact comes from a decision by the EU Court of Justice (ECJ) that has effectively eliminated Safe Harbor as an option for EU-US data transfers.

EU RESTRICTIONS ON DATA FLOWS TO THE US

As we have reported in the past, the EU Privacy Directive (Directive 95/46/EC) prohibits the exporting of personal data out of the EU to other countries unless those countries' laws provide "adequate protection" for personal information, with the EU determining what constitutes adequacy. The US privacy laws have historically not been viewed as providing adequate protection, which made US-EU transfers of information difficult. Companies receiving information formerly had four options, they could: (1) enter into a transfer agreement using "model clauses"; (2) put in place binding corporate rules (which must be approved by an EU data protection authority); (3) get consent from the individual (this option is not always available, however); or (4) participate in a special EU-US "Safe Harbor" Framework that the European Commission determined to be adequate in Decision 2000/250. With this new decision, Safe Harbor is now off the table.

SCHREMS FILES SUIT: HOW WE GOT HERE

As EU citizens became increasingly concerned over US surveillance activities, an Austrian citizen filed suit in Ireland (*Schrems v. Data Protection Commissioner*) arguing that Facebook Ireland should not be permitted to send his information to the US. In particular, he feared that his information would fall into the hands of the US government. The Irish Data Protection Commissioner rejected Schrems' complaint, largely on the grounds that the EU Commission had already decided that the Safe Harbor Framework provided "adequate protection" for purposes of the EU Privacy Directive. Schrems appealed to the Irish High Court. While he did not specifically state as such in his appeal, he was effectively challenging the validity of the EU-US Safe Harbor Framework. The Irish High Court stayed the proceedings and asked the ECJ for a preliminary ruling as to whether the Irish Data Protection Commissioner could, in fact, look at the underlying adequacy of the EU-US Safe Harbor Framework, notwithstanding the EU's prior determination that it was in fact adequate.[1]

Yesterday, the ECJ issued its ruling, concluding that Decision 2000/250 is invalid (and the Safe Harbor program not adequate) for two key reasons. First, the ECJ found the decision invalid because it failed to take into account whether or not the United States "'ensures' an adequate level of protection by reason of its domestic law or its international commitments."[2] Second, the ECJ took issue with the decision because it improperly attempted to restrict the national authorities' powers to determine if a non-EU country provided adequate protection. The ECJ's ruling concludes that notwithstanding any EU-level decision, supervisory authorities (like the Irish Data Protection Commissioner) in Member States could examine claims in which individuals argued that the transfer of their data was going to a country that did not provide adequate protection.[3]

The ECJ noted that while the Irish Data Protection Commissioner can and should take cases that question the validity of an EU Commission decision—as here, where Schrems' claim questioned whether the EU Commission properly determined that the Safe Harbor Program was adequate—only the ECJ could actually invalidate such an EU Commission decision[4]. And in this ruling, the ECJ did just that.

THE IMPACT ON EU-US DATA TRANSFERS AND SAFE HARBOR PARTICIPANTS

This decision places a burden on companies who rely on Safe Harbor as the basis for personal data transfers. US companies indicate in their privacy policies and on the US Department of Commerce website their compliance with the Program's provisions. They still have statements about their compliance on their websites. Should they take such statements down? What should they do about their listing with the Department of Commerce? As of this writing, the US Department of Commerce continues to maintain the list of US companies that have self-certified their compliance on its Safe Harbor website: http://export.gov/safeharbor/. Will the Department of Commerce list come down? What about EU companies that have been exporting to US companies that participate in the Safe Harbor Program? These questions will no doubt be asked. As of yet, they have not been answered.

For now, it seems unlikely that Member States will take immediate action against companies that have transferred data while relying on the EU-US Safe Harbor Framework. Indeed, the Deputy Commissioner for the UK Data Protection Authority has indicated that the ICO "recognise[s] that it will take some time" for businesses that use Safe Harbor to review how they ensure that data transferred to the US is in accordance with the law. It similarly seems unlikely that the Department of Commerce will take down its listing of Safe Harbor participants. Instead, discussions to find a solution are reported as ongoing between the US and EU.

NEXT STEPS FOR THOSE MAKING EU-US DATA TRANSFERS

In the immediate future, EU-based companies transferring data into the US may seek to have the US recipients of personal data execute model contracts, even if the US company has indicated its participation in the Safe Harbor Program. US companies should be prepared for such a request. US companies relying on Safe Harbor should thus begin to explore alternate approaches to obtain personal data from the EU.

TIP: We anticipate this decision will be highly scrutinized and reported on in the coming weeks, with its impact on US-EU commerce hotly debated. Negotiated solutions between the US and EU may also be forthcoming, although a political solution is unlikely to be in place soon. For now, companies who relied on Safe Harbor as their method of transferring personal data from the EU to the US will want to consider putting in place an additional method—like a model contract or binding corporate rules—to avoid the exposure to a potential Member State enforcement action.

---

[1] The exact wording of the Irish High Court's questions read as follows: "(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding? (2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?" *Schrems v. Data Protection Commissioner*, Case C 362/14 [2015], para 36.

[2] *Id*, paras. 97 and 98.

[3] The exact wording of the ruling reads as follows: "(1) Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of

Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection. And (2) Decision 2000/250 is invalid." Id., para. 107.

4 "Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves" *Id*, para. 62

6 Min Read

Related Locations

Brussels | Charlotte | Chicago | Houston | London | Los Angeles | New York | Paris | San Francisco | Silicon Valley | Washington, DC

Related Capabilities

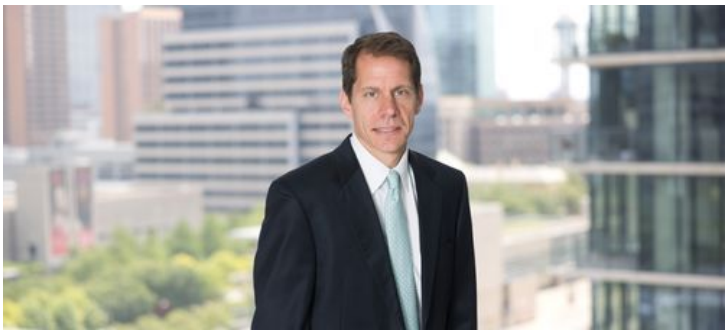
Privacy & Data Security | Intellectual Property

Related Regions

Europe | North America

Related Professionals

W. Gordon Dobie



John Rosenthal

Mary Katherine Kulback

Cardelle Spangler

Sara Susnjar

Alessandra Swanson

© 2025 Winston & Strawn LLP.