Published on *The National Law Review* https://natlawreview.com

European Court of Justice Invalidates U.S.-EU Safe Harbor Agreement

Article By:

Brian J. McGinnis

Brendan W. Miller

Negotiated under the European Commission's Data Protection Directive, the U.S.-EU Safe Harbor allowed United States companies to self-certify compliance with European Union (EU) data protection law standards allowing for the transfer of personal data from the EU to the U.S. without interruptions in business dealings and the risk of facing prosecution by EU data protection authorities. Prior to the Safe Harbor's invalidation on October 6, more than 4,500 U.S. companies relied on the Safe Harbor to ensure adequate compliance with the directive in personal data transfer. With the invalidation of the Safe Harbor, the future of cross border transfers between the EU and U.S. is very much in doubt. However, it is clear that companies must take immediate action to ensure their EU-U.S. personal data transfers are compliant with European data protection law.

Overview

On October 6, the European Court of Justice (ECJ) invalidated the Safe Harbor privacy pact between the U.S. and the European Union. Generally, data privacy laws in the U.S. are seen to lag behind the stricter and clearer requirements of EU data protection law. The Safe Harbor was a result following the EU's Data Protection Directive of 1995, which states that transfer of an EU citizen's personal data from any EU member state to a country outside the EU (third country) may only take place if the third country ensures an "adequate" level of privacy protection. The European Commission may find an adequate level of protection by way of a third country's domestic law or international commitments. Not long after the directive passed, the European Commission found the U.S. did not provide adequate levels of protection. Due to this finding, the EU and the U.S. negotiated the Safe Harbor agreement in 2000, allowing U.S. companies to certify that the protections they do provide are equivalent to the requirements under the directive. Many companies involved in the cross-border transfer of personal data from the EU to the U.S. relied heavily on the Safe Harbor to ensure the transfers were compliant with European data protection law. Through a series of revelations, EU citizens began to doubt the safety of their personal data and eventually challenged the Safe Harbor agreement, leading to its invalidation by the European Court of Justice.

The Safe Harbor

Self-certification under the Safe Harbor removed many of the hurdles faced by U.S. companies attempting to transfer data from EU member states under the directive – rather than having to comply with each individual member state's directive guidelines to transfer data, a U.S. company was able to self-certify and bypass individualized compliance. As of October 6, more than 4,500 U.S. companies relied on the U.S.-EU Safe Harbor agreement to make personal data transfers from the EU. Oversight of the Safe Harbor was delegated to the Federal Trade Commission and the Department of Commerce with minimal oversight by the European Commission. After being in effect for nearly 15 years, Safe Harbor compliance by U.S. companies was rarely questioned or enforced by the FTC or the Department of Commerce. Many viewed the Safe Harbor as merely a "promise" of compliance by the U.S. which turned into a free-for-all in regards to data transfers. The lack of attention and oversight by U.S. authorities, along with revelations regarding U.S. government surveillance, eventually led to the recent case in which the European Court invalidated the Safe Harbor.

The European Court of Justice's Decision

The legal case began in 2013 following Edward Snowden's publications regarding mass government surveillance by the NSA. These disclosures ignited concerns that EU data stored by U.S. companies, including Facebook, was subject to surveillance by the U.S. government that would be deemed illegal in Europe. Maximillian Schrems, an Austrian citizen and Facebook user, filed a complaint with the Irish Data Protection Authority and argued that U.S. government surveillance activities did not provide adequate protection of EU citizens' data being transferred to third countries. Schrems appealed to the European Court of Justice and challenged the very framework of the Safe Harbor.

The ECJ found that the European Commission's 2000 decision declaring the adequacy of the Safe Harbor privacy protections is invalid. The Court reasoned that the U.S. allows large-scale collection and transfer of personal data with no means of redress or effective judicial protection for EU citizens. The court stated that the Safe Harbor therefore lacked the requisite guarantees of privacy protection and its later implementation did not satisfy the requirements of the directive. As a result, the invalidation of the Safe Harbor agreement is effective immediately.

Individual EU member states will now implement their own data transfer regulations and conduct oversight of data transfers through their own data protection authorities. Thus, a U.S. company attempting to transfer data out of multiple EU member states may have to comply with 20 plus different sets of national data-privacy regulations. This also enables each of the member states to immediately suspend data transfers within their borders that were previously allowed under the Safe Harbor.

Actions for Consideration

Companies that wish to transfer personal data from the EU to the U.S., or that have used the U.S.-EU Safe Harbor as their primary compliance basis for EU-U.S. personal data transfers now find themselves asking: "What do we do now?"

In the wake of the Schrems ruling, unfortunately these answers are unclear. What is clear, however, is that the ECJ's ruling dictates that companies should consider taking action to identify an alternate compliance basis for EU-U.S. personal data transfers as quickly as possible. Companies failing to take action immediately may find themselves in violation of various contracts, unable to enter into new agreements with prospective EU partners, and subject to the enforcement of European authorities for violation of European data protection laws.

Alternatives to the Safe Harbor have existed for some time under the directive. However, each are significantly more time and cost intensive than the Safe Harbor, and each alternative carries with it its own risks and problems. The primary alternatives include:

1. **Consent**: EU data protection laws allow the transfer of personal data from the EU to the U.S. where an individual has given their consent. Typically, an individual's consent to the transfer of personal data must be fully informed, explicit, voluntary and unambiguous to be valid. However, many European jurisdictions consider it difficult to obtain valid consent due to the level of consent required, especially if you seek such consent retroactively after an original agreement has been signed. In addition, many European Member States have determined even informed consent is inadequate to transfer employee data.

2. **Model Contract Clauses**: The European Commission has approved certain model contract clauses that may be incorporated into agreements between exporting and receiving entities that seek to ensure EU personal data is protected to EU standards outside of the EU. Companies wishing to rely on these standardized contractual clauses should consider negotiating (or re-negotiating) with each EU data exporter with which they do business to incorporate the appropriate model clauses into their agreements. The clauses are inflexible and must be adopted as provided to retain the pre-approval. Some member states require model clauses to be filed with, or even approved by, regulators, adding further time and cost to compliance. Further, many speculate that the model contract clauses could be subject to invalidation under the same theories that invalidated the Safe Harbor, bringing their long-term effectiveness into question.

3. **Binding Corporate Rules (BCRs)**: BCRs are an alternative compliance basis only for EU companies wishing to share personal data with U.S. companies that are a part of their same corporate group (intragroup companies). The process for implementing BCRs is the most time-consuming and difficult of the alternative options. BCRs must be reviewed and approved by the relevant EU Member State regulators prior to enactment and can take up to 18 months or more to implement. Like the model contract clauses, BCRs are also subject to challenge in light of the Schrems decision.

Companies wishing to transfer data from the EU to the U.S. must take immediate action to ensure they comply with the dramatically altered legal landscape surrounding cross-border transfers between the EU and U.S. Companies should first identify and prioritize their most critical data transfers and seek to attain or re-attain compliance by amending contracts and agreements, or by other valid compliance means. The ECJ's ruling will require companies to take a case-by-case, country-by-country look at each contract or agreement with a EU data exporter to ensure they are placing themselves in a defensible position in light of the invalidation of the Safe Harbor.

Companies should also stay informed of the developments in the area and consider a longer term solution to their EU data transfers. The European Commission and U.S. Department of Commerce have been working on a revamped "Safe Harbor 2.0" for more than two years, but have yet to come to a new agreement. The Schrems decision certainly places a renewed importance on these negotiations and many hoe that the partnership will result in a clearer set of guidelines for U.S. and EU companies in the months to come. However, this ruling shows that even then, any Safe Harbor 2.0 guidelines would on shaky ground until challenged and upheld by a subsequent ECJ decision.

Implications for Litigation

In addition, litigants face unique challenges from the invalidation of the Safe Harbor and the uncertainty surrounding a comprehensive permanent solution. Global commercial disputes often involve cross-border data transfers in the course of litigation; implications for eDiscovery and data management demand careful consideration and planning with legal counsel. Parties engaged in current or prospective litigation involving such cross-border data transfers should consider:

1. **Taking inventory of data transfers** relating to the litigation to determine the scope and nature of the current reliance on the Safe Harbor.

2. Assessing with legal counsel and data vendors **alternative mechanisms** to accomplish compliant data transfers, including those described above.

3. **Evaluating the scope of data** that is being requested for transfer. For purposes of the litigation, can data requests be reasonably limited so as to reduce or eliminate personal data issues?

4. Do the circumstances of the litigation and the data transfer allow for personal data to be adequately protected through **pseudonymization** (removal of an association with a data subject that allows data to be linked to the same person across multiple records or systems without revealing the identity of the person), **anonymization** (permanently and completely removing personal identifiers) or other **redaction methods** that comport with applicable privacy laws?

5. Monitor developments in Safe Harbor regulatory alternatives, to ensure data transfers are compliant.

National Law Review, Volume V, Number 282