THE
NATIONAL LAW REVIEW

Advocate General Of ECJ Rules EU Data Protection Authorities Can Investigate Complaints About Safe Harbor Programme

Morgan Lewis

Article By
Dr. Axel Spies
Pulina Whitaker
Matthew Howse
Gregory T. Parks
Morgan, Lewis & Bockius LLP
Law Flash

- Communications, Media & Internet
- Election Law / Legislative News
- Global
- Litigation / Trial Practice

- All Federal
- European Union

Monday, September 28, 2015

Data transfers can be suspended until investigation is complete.

In ***Maximillian Schrems v. Data Protection Commissioner*** (case C-362/14), the Advocate General ruled that EU data protection authorities do have powers to investigate complaints about the transfer of personal data to the United States by Safe Harbor-certified organisations and can, where justified, suspend data transfers until their investigations are complete.

Safe Harbor Programme

According to the European Commission, the United States is a country of "inadequate" data protection. The European Commission and the US Department of Commerce, therefore, agreed in the year 2000 to a self-certification programme for

US organisations to receive personal data sent from Europe. The self-certification programme provided that US organisations must certify that they adhered to standards of data processing that are comparable with EU data protection laws such that EU citizens' personal data was treated as adequately as if their data had remained within Europe. This Safe Harbor programme is operated by the US Department of Commerce and enforced by the Federal Trade Commission. Over 4,000 organisations have current self-certifications of adherence to Safe Harbor principles.

In the course of Irish litigation, a question was referred to the ECJ for a ruling on whether EU Data Protection Authorities can investigate data transfers to organisations with Safe Harbor certification. Yves Bot, Advocate General at the European Court of Justice (ECJ), said in his opinion released on 23 September 2015 that the Safe Harbor programme does not currently do enough to protect EU citizens' private data because personal data had been obtained by US authorities in the course of "mass and indiscriminate surveillance and interception of such data" from Safe Harbor-certified organisations. The Irish Data Protection Commissioner, therefore, had the power to investigate complaints about Safe Harbor-certified organisations and, if there are "exceptional circumstances in which the suspension of specific data flows should be justified", to suspend the data transfers pending the outcome of its investigation.

Key Findings from the Advocate General's Opinion:

"Th[e] findings of fact demonstrate, in my view, that Decision 2000/520 does not contain sufficient guarantees. Owing to that lack of guarantees, Decision 2000/520 has been implemented in a manner that does not satisfy the requirements of the Charter or of Directive 95/46."

"There is no independent authority capable of verifying that the implementation of the derogations from the safe harbor principles is limited to what is strictly necessary."

"The [EU] Commission ought to have suspended the application of Decision 2000/520."

"Although it was aware of shortcomings in the application of Decision 2000/520, the Commission neither suspended nor adapted that decision, thus entailing the continuation of the breach of the fundamental rights of the persons whose personal data was and continues to be transferred under the safe harbor scheme."

"I am therefore of the view that Decision 2000/520 must be declared invalid."

While the Advocate General's opinions are not binding, they are often followed by the ECJ. The decision of the ECJ is expected soon.

Recommendations to Improve the Safe Harbor Programme

In 2013, following much discussion in the EU about the Safe Harbor programme after Edward Snowden's revelations about the NSA's PRISM programme, thirteen recommendations were made to improve the Safe Harbor programme.

The key recommendations are as follows:

Self-certified companies should publicly disclose their privacy policies
Privacy policies on self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website
Self-certified companies should publish privacy conditions of any contracts they have with subcontractors (e.g., cloud computing services)
The Department of Commerce should indicate which companies are no longer current members of the programme
The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider
The Department of Commerce should monitor ADR providers more systematically
The Federal Trade Commission should enforce misuse of the safe harbor certification more rigorously and conduct general investigations into certified organisations' compliance with their privacy policies
Privacy policies should note when an organisation will apply national security or law enforcement exemptions to allow data to be shared with US authorities

A final decision on whether these recommendations will be implemented is still awaited from the EU.

Summary

Notwithstanding the debate over the last two years, many organisations still view the Safe Harbor programme as an appropriate standard in data protection for non-European businesses and consider the Safe Harbor-certification as being a mark of trust in their data protection processes. Organisations that transfer personal data from Europe to the United States using the Safe Harbor programme may be concerned about the potential disruption to international data flows if the ECJ follows the Advocate General's opinion and the organisation is subsequently investigated by a European data protection authority. One important issue that the ECJ must address is whether the European Commission and/or EU Data Protection Authorities are authorised to "suspend" Safe Harbor-certified data transfers. The European Commission is considering the above-mentioned recommendations to improve data protection measures under Safe Harbor. The ECJ should, therefore, be mindful not to create a patchwork of some (perhaps stricter) EU Data Protection Authorities suspending data transfers by certain organisations, while other Data Protection Authorities have no such objections about these same organisations. Under the proposed new General Data Protection Regulation, there will be a consistency mechanism that is designed to avoid such a situation.

It is also worth noting that nothing about this decision invalidates Safe Harbor as a mechanism to transfer data. It merely provides that a data protection authority investigating a specific organisation could, upon finding "exceptional circumstances",suspend that organisation's ability to transfer data under Safe Harbor pending investigation. If organisations remain in full compliance with their Safe Harbor obligations, they should have no reason to fear suspension of data flows.

Before blocking the data flows or "suspending" Safe Harbor, the European

Commission and the Data Protection Authorities should bear in mind that the US Government has made strides to block illegal data collections by law enforcement authorities (e.g., by the USA Freedom Act of 2015 or the Presidential Policy Directive 28). The Federal Trade Commission has also imposed penalties on various companies that were deemed not Safe Harbor-complaint by way of consent decrees.

For organisations with concerns that their Safe Harbor certification may be undermined by this ruling, there are other options to transfer personal data to the United States, including express consent and the use of Binding Corporate Rules or EU-approved model clause agreements.

Source URL: https://www.natlawreview.com/article/advocate-general-ecj-rules-eu-data-protection-authorities-can-investigate-complaints