6 October 2015

Practice Group(s):

Public Policy & Law

Privacy, Data Protection & Information Management

Telecom, Media and Technology

Did the ECJ Kill the Safe Harbor Framework on E.U.-U.S. Data Transfers?

By Etienne Drouard, Ignasi Guardans, Samuel R. Castic, and Claude Etienne Armingaud

The Facts

On October 6, 2015, the European Court of Justice ("ECJ") ruled in the *"Schrems"* case that U.S.-EU Safe Harbor framework on the transfer of personal data from Europe to the United States, was invalid.

For the past 15 years, this Safe Harbor framework gave privileged status to U.S. companies, allowing for such entities to "self-certify" that they complied with privacy standards negotiated between the European Commission and the United States Department of Commerce under the Clinton Administration in 1999, and were viewed as "adequate" by the EU. Effective immediately, today's ruling may force all of the 4,400 U.S. entities currently relying on the Safe Harbor to access the data of their EU partners and subsidiaries to seek alternate modes of data transfer, or to risk non-compliance with EU data protection requirements.

The Facts

Austrian privacy campaigner Maximilian Schrems originally formed his complaint before the Irish Data Protection Authority ("DPA") against Facebook's use of his data, and the transfer of data occurring between Facebook's Ireland entity and its U.S. parent company. According to the complainant, and based on Edward Snowden's revelations on mass surveillance, Facebook and other U.S. multinationals were, directly or indirectly, allowing U.S. national security agencies unrestricted access to EU citizens' data. Such unrestricted access could be construed as being in violation of the fundamental rights granted under the EU Data Protection Directive 95/46 (the "**Data Directive**"), currently under revision in the EU.

After the Irish DPA declined to investigate such concerns on the basis that the Safe Harbor implemented between the U.S. and Irish entities was exclusively overseen by the European Commission, the complaint was elevated before Europe's highest Court.

The Decision

The ECJ disagreed with the Irish DPA's interpretation, by stating that the existing provision "*does not prevent a supervisory authority of a Member State ... 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 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".*

In essence, this means that each EU member state DPA has the authority to hear complaints about the level of protection for personal data that other countries offer, and potentially to

second guess any determinations that the European Commission has made that those countries offer adequate protection.

In addition, the Court noted that *"legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law".*

Following the opinion of Yves Bot, the ECJ's Advocate General for the case, dated September 23, which notably stated that "*once personal data is transferred to the United States, the National Security Agency and other United States security agencies such as the Federal Bureau of Investigation are able to access it in the course of a mass and indiscriminate surveillance and interception of such data*", the Court invalidated the EU Commission decision 2000/520/EC of 26 July 2000 on the adequacy of the Safe Harbor framework to EU privacy standards.

The Reactions of the EU Institutions

The EC promptly reacted to the decision of the ECJ. In a press conference on the same day of the ruling, the First Vice-President of the EC, Frans Timmermans, and the Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, explained how the EC is planning to tackle the issues raised by the Court.

In particular, they clarified that the Commission has now three priorities, in light of the ECJ's ruling: (i) guaranteeing that the data of EU citizens are protected when transferred across the Atlantic, (ii) ensuring that data flow continues, and (iii) ensuring the uniform response on alternative ways to transfer data across the EU.

According to Commissioner Jourová , the data flow can continue under EU data protection rules which provide for other mechanisms of safeguards for international transfers of personal data (e.g. standard data protection clauses in contracts between companies exchanging data across the Atlantic or corporate rules for transfers within a corporate group) and the derogations under which data can be transferred (i.e. performance of a contract, important public interest grounds, vital interest of the data subject, or consent of the individual).

The EC is planning to provide clear guidance to national data protection authorities on how to deal with data transfer requests to the US, in the light of the ruling, and will put relevant information and contact points on its website. The guidance should guarantee a uniform enforcement of the ruling and more legal certainty for citizens and businesses.

The Chair of the European Parliament Civil Liberties Committee, Claude Moraes, has called for the immediate suspension of the Safe Harbor agreement, following the decision of the ECJ, and for its replacement by the Commission with a new framework for transfers of personal data to the US in compliance with EU law. The European Parliament had already advanced those requests more than once in the past.

Did the ECJ Kill the Safe Harbor Framework on E.U.-U.S. Data Transfers?

The Reaction of the United States Department of Commerce

The Secretary of the U.S. Department of Commerce, Penny Pritzker, promptly released a press release in response to the decision that expressed deep disappointment for the decision. The statement indicates that the decision *"creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy."* It further calls for the release of the updated Safe Harbor Framework *"as soon as possible."*

Secretary Pritzker's statement also indicates that the U.S. is prepared to work with the European Commission to address the uncertainty that this decision causes for U.S. and EU businesses so that businesses that *"have complied in good faith with the Safe Harbor and provided robust protection of EU citizens' privacy in accordance with the Framework's principles can continue to grow the world's digital economy."*

Immediate Impacts and Long-term Consequences

The ECJ decision will now be sent to the High Court in Dublin, in order for the national judge to use this new interpretative framework as a basis for deciding on Schrems' legal challenge for Facebook to be audited.

While the ECJ decision is of immediate application, the practical effect in a B2C setting will actually depend on the actions of the DPAs in each European Union member state, and others. Meanwhile, public outrage may lead to a wave of complaints and possible requests for interim action, such as injunctions before national courts. Such initiatives may notably be undertaken by the likes of complainant and privacy activist Mr. Schrems, and others who follow his lead.

Strictly speaking, only a decision from the European Commission has been invalidated — the Safe Harbor remains a voluntary mechanism adopted by the United States under the supervision of the U.S. Federal Trade Commission ("FTC") or Department of Transportation ("DoT"). Accordingly, companies that have certified as compliant with the Safe Harbor are still subject to FTC or DoT jurisdiction, but compliance with the Safe Harbor Framework is no longer assumed by European authorities to offer an adequate level of protection.

The consequence of this ECJ decision lies in the fact that each national DPA now has the power to control the conformity of a data transfer not only to the Data Directive, but also to the Safe Harbor framework. Therefore, the compliance of the U.S. data importer with the Safe Harbor Framework may now be scrutinized by both the FTC and DoT (as before), and each local DPA.

From a B2B point of view, this decision will, without doubt, disrupt the ongoing negotiations with European business customers, who might threaten to interrupt the delivery of goods or services and seek redress for noncompliance until their providers establish alternative grounds to transfer data to the United States in accordance with the requirements of the Data Directive.

Next Steps

While the Safe Harbor certification of each U.S. entity may now be scrutinized by each local EU DPA, from an EU law perspective, alternate modes of data transfers, such as **Data**

Did the ECJ Kill the Safe Harbor Framework on E.U.-U.S. Data Transfers?

Transfer Agreements based on the EU Commission Model Clauses (a fixed contractual template regulating the transfer of data from one EU data exporter (or more) to a non-EU data importer (or more)) or **Binding Corporate Rules** ("BCR", an ad-hoc set of rules governing the processing of personal data within the various entities of a given group of companies)), may still be relied upon.

The BCR approach involves potential risks to both U.S. companies and European corporate affiliates, including the following:

- If the Safe Harbor certification of a U.S. company is deemed invalid by a DPA, this European DPA may initiate sanctions against any EU exporter making data available to this U.S. data importer. If this U.S. data importer has no physical or commercial presence in EU territory, no sanction may be enforced against it by a EU DPA.
- If, for the security of their data transfers from Europe, the U.S. importers execute Data Transfer Agreements with their EU counterparts, the joint-liability regime of the European Model Clauses will make the EU data exporter bear the whole of the actual liability.

On the one hand, Model Clauses are easily executable, but do not provide much flexibility. In addition, their adoption involves legal risk due to their pass-through liability and audit requirements, and is not always feasible due to the need to execute clauses with any sub-processors that will have access to the personal data transferred. On the other hand, BCR are time consuming and potentially expensive to implement, but may offer a tailor-made solution for a given group of entities.

U.S. companies should carefully explore the risks and benefits that data transfers using the Model Clause and BCR approaches offer, and may also wish to re-examine business practices to avoid exposure to the legal risks that transfers of personal data outside of the EU involves. A re-examination and change in data transfer practices could help mitigate the risks that the Model Clause and BCR approaches have under EU law, as well as potential risks that agreeing to European-style data protection expectations might have if tested in litigation in U.S. courts.

The draft Data Protection Regulation currently being discussed in the EU appears to maintain both the Model Clause and BCR mechanisms, which also offer the advantage of regulating data transfers worldwide and not solely to the United States.

We may reasonably doubt that the ECJ's intention was to sanction EU companies that transfer data outside of the EU under the Safe Harbor framework. Notwithstanding, this may be the final outcome of its decision.

There is little doubt that this decision will have a political impact, should the Obama administration elect to carry this issue forward within the Trans-Atlantic talks notably surrounding the adoption of the TTIP, once the draft Data Protection Regulation is adopted in the EU before the end of 2015.

Did the ECJ Kill the Safe Harbor Framework on E.U.-U.S. Data Transfers?

If you would like our Global Data Protection Team to help assess and mitigate the specific circumstances applicable to your organization, please contact our team members:

Paris:

Etienne Drouard
etienne.drouard@klgates.com
+33.(0)1.58.44.15.12

Claude-Etienne Armingaud
Claude.Armingaud@klgates.com
+33.(0)1.58.44.15.16

Brussels:

Ignasi Guardans
Ignasi.Guardans@klgates.com
+32.(0)2.336.1949

Berlin:

Friederike Gräfin von Brühl
friederike.bruehl@klgates.com
+49.(0)30.220.029.415

London:

Arthur Artinian
arthur.artinian@klgates.com
+44.(0).20.7360.8207

Andrew Danson
andrew.danson@klgates.com
+44.(0).20.7360.8153

Andrew Gilchrist
andrew.gilchrist@klgates.com
+44.(0).20.7360.8148

Washington, DC:

Bruce Heiman
bruce.heiman@klgates.com
+1.(202) 661-3935

Seattle:

Holly Towle
holly.towle@klgates.com
+1.(206) 370-8334

Sam Castic
sam.castic@klgates.com
+1.(206) 370-6576

Did the ECJ Kill the Safe Harbor Framework on E.U.-U.S. Data Transfers?

Pittsburgh:

Susan Altman
susan.altman@klgates.com
+1.(412) 355-8261

Melbourne:

Cameron Abbott
cameron.abbott@klgates.com
+61.3.9640.4261