www.tlgdc.com
@TechLawGroup

TELECOMMUNICATIONS
SNAP UPdate℠

January 27, 2016 *by*: *Matthew R. Friedman, Esq.*

European Court of Justice Strikes Down US-EU Safe Harbor Agreement: Action Creates Legal Issues and Uncertainty for the Cloud Services Economy

Washington, DC: With the rise of the cloud economy, the transfer of data between the United States and Europe has become increasingly commonplace, and even necessary for many businesses. European Data Directive 95/46/EC, however, adopted by the European Parliament and the Council for the European Union over twenty years ago, provides substantial limitations on the movement of such data. Indeed, personal data from the European Union may only be transferred to third party countries (such as the United States) if that country ensures an adequate level of protection of the data. Any data transfer in violation of the European Data Directive is illegal.

For fifteen years, a US-EU Safe Harbor Agreement provided a framework under which US companies engaging in the transfer of data from the European Union could certify that they complied with Directive 95/46/EC, become part of the Safe Harbor program, and thus legally transfer such personal data. However, on October 6, 2015, the European Court of Justice ("ECJ") – the highest court in Europe – struck down the US-EU Safe Harbor Agreement, immediately making illegal all transfers of personal data from the EU to the US that relied only on the provisions of the Safe Harbor Agreement for their legality. As a result, over 4500 companies relying upon the US-EU Safe Harbor Agreement are left between a rock and a couple of hard places – either continue to engage in business as usual and risk prosecution, stop data transfers from the EU to US altogether, or come into compliance with an alternative compliance mechanism. While companies such as Facebook and Amazon, which have massive data infrastructures and storage

needs, receive the most media attention, any company or entity engaging in data transfers and/or processing between the US and the EU – even if just for hosting EU data on a US server or for obtaining data for an employee that may work in the EU – must comply with European Data Directive 95/46/EC.

The ECJ order also leaves other players in the cloud economy, such as agents, in a similar, potentially perilous position as the data transfer and cloud services agreements they promote may now contemplate, and indeed even require, illegal data transfers. Such illegality may not only be a basis for termination or rescission of such agreements, but may also open the door for lawsuits by the Federal Trade Commission and other regulatory bodies who are empowered to prosecute against persons and entities engaging in unfair and deceptive practices that violate consumer privacy.

Talks are currently underway between representatives of the US and the EU to develop a "Safe Harbor 2.0" framework that would provide an alternative mechanism for ensuring the legality of data transfers from the EU to the US. The details of such a framework are currently unknown, but the release of its terms is anticipated to occur early next week, coinciding with the deadline set by Europe's data protection authority – the Article 29 Working Group - for such a decision. In the event a solution is not reached by this deadline, the Article 29 Working Party has stated an intention to "take all necessary and appropriate actions, which may include coordinated enforcement actions." As a result, the potential of quick and serious enforcement actions is high, and even if an adequate solution is developed, there will likely be very little time to implement any required changes in any non-compliant data transfer protocols and procedures that companies are currently utilizing.

While the previous Safe Harbor Agreement served as the primary mechanism for ensuring the legality of transfers of personal data from the European Union to the United States, there are other ways, including binding corporate rules and model contracts, that can be implemented to ensure the legality of data transfers. Binding corporate rules, often utilized by multinational companies, set forth a company's global policy regarding international transfers of personal data, as well as any threshold conditions. Model contracts can be drafted to include specific language that the EU has certified as sufficient to protect the privacy interests of European citizens. To be compliant, each and every contract covering any transfer of personal data from the EU to the US must contain this language, and such transfers must be made in compliance with the established procedures.

TLG will issue a further SnapUPdate promptly following the release of the Safe Harbor 2.0 framework. In the interim, if you have questions about these issues, or if we may otherwise be of assistance to you, please feel free to contact us. We are also pleased to assist you in the development of corporate rules and/or in the drafting of appropriate contract language that ensures compliance with the newly adopted Safe Harbor 2.0 framework, once and if adopted.

Additional information on this issue and the latest telecom news is available through the Technology Law Group Twitter account, @TechLawGroup, as well as through TLG's TelecomLaw Center and Telecom Counsel Network LinkedIn groups.