LOEB & LOEB LLP

Privacy

OCTOBER 2015

No Safe Harbor for EU-U.S. Data Transfers

by Ieuan Jolly, Partner

In a landmark decision with immediate repercussions for both American and European companies, Europe's highest court, the Court of Justice of the European Union (CJEU), ruled that the EU-U.S. Safe Harbor framework enabling data transfers of personal data between the EU and U.S. is invalid. The decision means that thousands of American companies that handle the personal data of European citizens may no longer rely on Safe Harbor certification to legitimize data transfers from the EU to the U.S. These companies — and EU-based businesses and their affiliates that transfer personal data to the U.S. in the course of doing business — must now implement other mechanisms for data transfers, or risk claims that these transfers are unlawful.

Below, we outline the commercial implications of the decision for cross-border data transfers from Europe to the U.S., identify which companies will be affected and provide some immediate steps that companies can take to achieve continued compliance for their international data transfers.

Background to the Ruling

The EU Data Protection Directive permits the transfer of personal data to countries outside the European Economic Area only if the country to which the data is transferred offers an adequate level of protection for that data. The European Commission does not consider that the U.S. has privacy laws that offer this level of protection. "Safe Harbor" was originally created by the European Commission and the U.S. Department of Commerce as a framework that would enable U.S.-based companies to overcome the restrictions on transfers of personal data from Europe by self-certifying that their data protection practices adequately address the European Commission's core privacy principles.

The CJEU's landmark decision follows a dispute between an Austrian citizen and the Irish Data Protection Authority, in relation to concerns about the transfer of the claimant's personal data by Facebook to the U.S. under the Safe Harbor framework. The claimant focused on the fact that the privacy laws of the U.S. do not offer sufficient protection against such surveillance by the U.S. government, particularly in light of revelations made by Edward Snowden concerning the surveillance activities of the U.S. intelligence services. The CJEU was asked to determine whether the Data Protection Authorities of EU Member States are bound by the European

Commission's ruling on the adequacy of the data protections afforded by the Safe Harbor framework.

In its decision, the CJEU went beyond this specific question and declared that the Safe Harbor framework does not provide an adequate level of protection for personal data transferred from the EU to the U.S., identifying a number of factors, including that the Safe Harbor could not prevent access by U.S. intelligence authorities to personal data transferred from the EU, and because it provides EU citizens with limited means of judicial redress in the U.S.

Who Is Impacted and How?

The ruling has an immediate impact on a wide range of companies, with four groups of businesses being high on the watch list:

- U.S.- based service providers certified under Safe Harbor to receive personal data from European customers will need to provide alternative assurances for those customers to be able to use their services lawfully. This would include vendors providing data hosting, storage, cloud solutions, SaaS, data analytics and social networks, and a range of other businesses that have built their data transfer models on Safe Harbor.
- EU-based companies on the buy-side that have engaged the services of U.S.-based companies will need to consider on what basis they can lawfully transfer personal data to the U.S., now that transfers of such data to the U.S. previously relying on Safe Harbor would be considered unlawful.
- EU-based data processors, such as cloud storage companies, that would typically host some or all of their data in the U.S. and that had previously relied on Safe Harbor to effect transfers of personal data to the U.S. will need to consider alternative options.
- Multinationals that had previously relied on their Safe Harbor certification to legitimize intragroup transfers of personal data from EU subsidiaries to their U.S. parent company or other U.S.-based affiliates will need to implement an alternative mechanism.

What Alternative Options Are There to Safe Harbor?

The (i) focus of your business, (ii) nature of the data transfers you engage in and (iii) entities involved in the data transfer (e.g., service providers, partners, intracompany groups, etc.) will determine which solution is most appropriate, but possible alternatives to achieve compliance with the EU rules on data transfers include:

- Incorporating EU Commission-approved Standard Contractual Clauses (SCCs) — a special type of data-processing agreement — as part of standard terms and conditions governing business relationships.
- Developing "Binding Corporate Rules" for the transfer of personal data between entities within an international corporate group that agree to detailed data-sharing protocols that are reviewed and agreed on by various Data Protection Authorities (DPAs).
- Obtaining the consent of EU data subjects to the transfer of their personal data to the U.S. (however, this option is often logistically difficult and needs to be used with care — particularly in the context of transferring HR data — and is likely to be scrutinized by national DPAs and courts).
- Keeping data within the EU by using a local data-processing facility or EU-based group entity as the customer-facing service provider.

What Steps Should You Take?

Companies should consider the following measures if their data transfers are impacted by the Safe Harbor decision:

- As a general matter, initiate a complete audit of data transfers to identify transfers that were undertaken in reliance on the Safe Harbor.
  - Review all entities with which you engage in EU-U.S. data transfers — including nonaffiliated companies, business partners and intracompany groups — and see what data transfer scheme is used by those entities.
  - Review the data transfer mechanisms you rely on to transfer personal data, and identify any that are based on the Safe Harbor.
  - Identify the types of personal data and use cases for those datasets that you are transferring to the U.S. Prioritize addressing the transfers of high volumes of personal data and sensitive personal data (e.g., health information, financial information, information about political or religious beliefs or sexual preference).
- For EU-based business customers that have engaged U.S.-based service providers:
  - Review contracts with third-party vendors to determine which contracts include data transfers under Safe Harbor certification, and consider appropriate alternatives for data transfer.
  - Consider whether you can force the U.S. service providers to sign up to the SCCs, or what rights you have under your contract to require the U.S. service providers to comply (e.g., consider provisions governing compliance with laws, change control, liability and termination provisions).
- For U.S.-based service providers that receive personal data from EU businesses under the Safe Harbor:
  - Consider what data transfer mechanism is the most appropriate for your business. Can you enter into the SCCs? Could you provide the services using servers within the EU or without transferring personal data outside the European Economic Area?
  - Review your contracts to understand the implications of not being able to rely on Safe Harbor for data transfers. Consider whether this development puts you in breach of specific contractual obligations or gives the customer rights to force you to adopt alternative data transfer mechanisms, or allows the customer to terminate the contract.
- For businesses that are considering engaging a new service provider that will receive personal data in the U.S. from the EU, make sure that they are not relying on their Safe Harbor certification to legitimize that transfer. You should include in the contract appropriate compliance methods, or use the SCCs to effect the transfers.
- For multinationals requiring intragroup transfers of HR data, consider implementing intragroup agreements and Binding Corporate Rules. Alternatively, if operationally feasible, consider whether you can process employee data within the EU or locate a centralized HR repository within the EU.

Cross-border data transfers are a complex area requiring careful consideration of international data protection frameworks and commercial contract analysis. For tailored advice on the impact of the EU ruling on your business and advice on next steps you should take, please contact Ieuan Jolly at ijolly@loeb.com.

Advanced Media and Technology Practice

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ELIZABETH J. ALLEN	EALLEN@LOEB.COM	312.464.3102
AMIR AZARAN	AAZARAN@LOEB.COM	312.464.3330
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MEG CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
ALESON CLARKE	ACLARKE@LOEB.COM	310.282.22240
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
CAROL M. KAPLAN	CKAPLAN@LOEB.COM	212.407.4142
ELIZABETH H. KIM	EKIM@LOEB.COM	212.407.4928
JANICE D. KUBOW	JKUBOW@LOEB.COM	212.407.4191
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
SCOTT S. LIEBMAN	SLIEBMAN@LOEB.COM	212.407.4838
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ELISABETH O'NEILL	LONEILL@LOEB.COM	312.464.3149
SUE K. PAIK	SPAIK@LOEB.COM	312.464.3119
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
MEREDITH SILLER	MSILLER@LOEB.COM	310.282.2294
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960