Insight

IN-DEPTH DISCUSSION

OCTOBER 7, 2015

What Does the European Court of Justice's Invalidation of the U.S.-EU Safe Harbor Framework Mean For U.S.-Based Multinational Employers?

BY PHILIP L. GORDON AND TAHL TYSON

In a landmark decision that will dramatically affect thousands of U.S. companies that transfer personal data from the European Union ("EU") to the United States, the European Union Court of Justice ("ECJ") yesterday invalidated the Safe Harbor Framework, which had permitted U.S. companies to comply with EU restrictions on the transfer of personal data outside the EU.

More than 4,000 companies, primarily U.S.-based multinationals, currently rely on the Framework, an agreement forged years ago between the U.S. Department of Commerce and the European Commission (the "Commission") to permit the transfer of personal data. The ECJ's decision, dated October 6, 2015, throws current procedures by these companies into question, and almost certainly will spur ongoing negotiations between the U.S. and the EU to develop a replacement. In the meantime, U.S.-based multinational employers will need to consider their alternatives, as discussed in detail below, to lawfully transfer the personal data of EU employees to the United States.

Brief Overview of the U.S.-EU Safe Harbor

The European Union Data Protection Directive (the "Directive") is the EU-level law governing the protection of "personal data," which encompasses any individually identifiable information about a natural person. The Directive generally prohibits the transfer of personal data to a country outside the EU unless the receiving country ensures an "adequate level of protection" for the personal data. The Directive also provides that the Commission may find that a third country ensures an adequate level of protection either based on that country's (a) national data protection laws, or (b) international commitments.

In 2000, the Commission issued a determination (the "Safe Harbour Decision") that while U.S. national law did not ensure an adequate level of protection for personal data according to European standards, the Safe Harbor Framework, which had recently been negotiated between the Commission and the Commerce Department, met that standard. The Safe Harbor Framework had been negotiated to bridge the differences in legal frameworks and provide a streamlined

and cost-effective means for U.S. organizations to satisfy the Directive's "adequacy" requirement. Under the Safe Harbor Framework, U.S. businesses wishing to receive personal data from the EU were required to (i) post a Safe Harbor Privacy Policy in which they represented their intention to adhere to the seven Safe Harbor Principles designed to protect the data, (ii) submit a self-certification form through the Commerce Department's Safe Harbor web site, and (iii) pay the required fee. The Federal Trade Commission was primarily responsible for enforcing the Safe Harbor Framework.

Legal Challenge to the Safe Harbor Framework

In 2012, a young Austrian by the name of Max Schrems was studying law for a semester at Santa Clara University, when he started intensive data privacy activism focused on Facebook's handling of the personal data of its EU users. Among his many actions, Schrems lodged a complaint with the Irish Data Protection Commissioner on the grounds that Edward Snowden's leaks of data gathered by U.S. intelligence through the "Prism Program" proved that the United States fails to provide sufficient protection for personal data transferred from the EU against covert government surveillance (notably by the National Security Agency). The Irish Data Protection Commissioner ("DPC") resisted and ultimately rejected Schrems' complaint, primarily on the ground that as a national level data protection authority its hands were essentially tied by the Commission's adequacy determination (and that Schrems' complaint was "frivolous and vexatious.").

The case then went to the High Court of Ireland, which agreed that there was nothing for the DPC to investigate given that the Commission already had determined that the Safe Harbor regime provided adequate data protection. The High Court referred to the ECJ the issue whether the Commission's adequacy determination remained valid.

Next, the Advocate General, who is appointed by the ECJ, issued a non-binding opinion recommending that the ECJ (i) invalidate the Commission's Safe Harbor adequacy determination because of alleged indiscriminate surveillance by the U.S., and (ii) hold that, because of the importance of national authorities in the protection of individuals' data protection rights, national regulators can investigate an EU citizen's complaint and block a data transfer where the regulator is satisfied that the third country will not adequately protect the fundamental data protection rights of individuals.

The ECJ's Decision Invalidating the Safe Harbor

As the starting point for its October 6 decision, the ECJ construed the Directive's standard requiring that a third country's laws "ensure an adequate level of protection" for personal data. According to the ECJ, this standard requires that the third country's laws and international commitments provide a level of protection for "the private lives and basic freedoms and rights of individuals" that is "essentially equivalent to that guaranteed within the European Union by virtue of [the] Directive." The ECJ scrutinized the Safe Harbor Framework and found it failed to meet this standard with respect to enforcement, access to personal data by intelligence agencies, and the ability of EU citizens to enforce their rights.

First, the ECJ implicitly questioned the rigor of the Federal Trade Commission's enforcement of the Safe Harbor. The ECJ stated that because the Safe Harbor relied on self-certification, the viability of the Framework depended on "effective detection and supervision mechanisms" to protect fundamental rights "in practice." However, the ECJ pointed to a finding in a report on the Safe Harbor prepared by the Commission in 2013 in the wake of the Snowden's disclosures and presented to the European Parliament that "in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles."

The ECJ also expressed serious concern that the Safe Harbor permitted U.S. intelligence agencies to collect substantial quantities of personal data of EU citizens from companies that had certified to the Safe Harbor, including many of the most well-known Internet companies. In the ECJ's words, the Safe Harbor Framework "lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements…" From the ECJ's perspective, the collection of EU personal data by U.S. intelligence agencies, as revealed by Snowden's leaks, demonstrated that this structural flaw undermined the fundamental rights of EU citizens. In this regard, the ECJ pointed to the following finding in the Commission's 2013 report: "'all companies involved in the PRISM programme, and which grant access to U.S. authorities to data stored and processed in the [United

States], appear to be Safe Harbour certified' and that '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'."

Finally, the ECJ relied on its conclusion that the Safe Harbor Framework did not provide EU residents with sufficient means to exercise their data protection rights under the Directive or to obtain judicial review of alleged violations. In this regard, the ECJ noted the finding in the Commission's 2013 report that the Safe Harbor provides "no opportunities for either EU or U.S. data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the U.S. surveillance programmes."

What Does the ECJ's Decision Mean for U.S. Multinational Employers Certified to the Safe Harbor?

For years, U.S. multinational employers have centralized their global human resources data in databases located in the U.S. to facilitate global workforce management. With the advent of cloud computing, many of these multinational companies have turned to cloud service providers—including, for example, human resources information systems ("HRIS") providers, payroll administrators, and on-line applicant tracking providers—located in the United States to house these centralized databases. To the extent these employers have relied on the Safe Harbor Framework to "ensure an adequate level of protection" for the personal data of EU applicants and current and former employees, the ECJ's decision obviously means employers will need to adopt alternative measures to meet the required standard for the protection of personal data received from the EU.

Alternatives to Safe Harbor Certification

At this point, two principal alternatives are available, each of which presents its own challenges. First, employers can consider using the "Standard Contractual Clauses" ("SCCs") approved by the European Commission. These clauses are embedded in a data transfer contract between the EU-based subsidiary (the "data exporter") and the U.S. parent corporation ("data importer"). Second, employers could consider relying on binding corporate rules ("BCRs").

Standard Contractual Clauses

SCCs (also referred to as "Model Clauses") can be unwieldy, administratively burdensome, and slow to implement. The parties to these agreements cannot modify the SCCs, in any respect, to address any factual circumstances specific to their relationship. In addition, the parties are required to complete a form appendix to the SCCs that describes the data transfer in substantial detail, including the categories of data to be transferred and the purposes for which the transferred data will be processed. When the data importer needs to import additional categories of personal data or use the personal data transferred for new purposes, the appendices to the data transfer agreements must be amended. When a U.S. multinational has a large number of EU subsidiaries, managing these agreements and the amendments to them can be administratively burdensome.

Adding to the potential burden, the data protection authorities in approximately a dozen EU Member States— including, for example, Austria, Belgium, France, Poland, and Spain—may require submission and approval of the data transfer agreements before the local subsidiary can rely on them to transfer personal data. For many U.S.-based human resources professionals under pressure to implement a global HRIS on a short timeline and a limited budget, this waiting period could pose a substantial impediment to timely implementation.

Binding Corporate Rules

Binding corporate rules provide another alternative mechanism to the Safe Harbor for transfers of personal data within a corporate group. BCRs involve the development and implementation of a uniform set of rules that are binding on all members of the corporate group, regardless of location, and that provide the high level of protection for personal data required by the Directive.

While BCRs may initially appear to be a ready-made solution for U.S. multinationals that previously relied on Safe Harbor certification, they likely will not provide the answer for most companies. Notably, since the Commission first approved BCRs in November 2004, fewer than 100

companies globally and fewer than 30 in the U.S. have implemented them. Those organizations that have implemented BCRs are among the largest, richest and most sophisticated U.S. corporations. BCRs likely have been selected by so few organizations (as compared to the more than 4,000 organizations certified to the Safe Harbor) because of the onerous approval process. The data protection authority of each country where the U.S. organization has a subsidiary with employees is entitled to an opportunity to review and comment on the BCRs.

This review and approval process can require substantial resources to navigate and routinely takes more than one year to complete. Moreover, with the invalidation of the Safe Harbor, many data protection authorities likely will see a spike in requests for approval of BCRs, resulting in additional delay. With the low cost and ease of trans-Atlantic telecommunications, many smaller U.S. companies are now multinational employers. These companies typically will not have the internal resources, financial capital, or time to complete the BCR review and approval process.

Safe Harbor Replacement?

Since the Commission issued its 2013 report criticizing the Safe Harbor, the Commission and the Commerce Department have been negotiating modifications to the then-existing Framework. According to media reports, those negotiations have made significant progress. Because that the U.S. and the EU are each other's largest respective trading partner and given the need for a relatively easy and inexpensive means for lawfully transferring personal data between the trading blocs, the negotiators likely will view the ECJ's decision as a spur to expedite completion of their negotiations. Moreover, the ECJ's detailed criticism of the now-invalidated Safe Harbor effectively created a roadmap for a "replacement Safe Harbor" that will meet the ECJ's standards.

To be sure, progress toward the completion of a "replacement Safe Harbor" is shrouded in the typical secrecy of diplomatic negotiations. However, the Commission or the Commerce Department may soon issue a statement providing some clarity on the anticipated completion of their negotiations. In the meantime, U.S. multinational employers will need to weigh the risks of a wait-and-see approach against the costs of implementing an available alternative.

The "Derogations"

As with most legal rules, the Directive sets out several exceptions, referred to in EU parlance as "derogations," to the general rule that personal data cannot be transferred to a third country unless that country "ensures an adequate level of protection" for personal data. The only two derogations that potentially apply in the employment context are (a) transfers with the unambiguous consent of the data subject, *i.e.,* the employee; and (b) "the transfer is necessary for the performance of a contract between the data subject and the controller," *i.e.,* the EU-based employer. Unfortunately, neither of these derogations is likely to provide a feasible solution.

Before the Safe Harbor Framework was implemented and for several years after, many U.S. multinationals relied on employees' consent to legitimize cross-border data transfers. However, EU data protection regulators have expressed their strong disfavor of reliance on this derogation in the employment context. According to these regulators, for consent to be valid, it must be "freely given"; however, because of the hierarchical nature of the employment relationship, employees cannot freely give consent as a matter of law.

While consent likely is not a viable solution for transfers of employee data, it may be a viable option for transfers of the personal data of job applicants. Job applicants are not yet in a hierarchical relationship with the prospective employer. In addition, job applicants can freely give consent because they have the choice not to apply for a position with an employer who will transfer their personal data to the United States.

Importantly, employers who plan to rely on consent to transfer applicants' data will be required to provide applicants with robust notice—for example, through an online applicant privacy policy—that complies with all applicable EU data protection laws. In addition, in order for applicants' consent to be "unambiguous," the employer will need to provide a means for the applicant to affirmatively express acceptance of terms of any privacy notice.

Although many EU subsidiaries of U.S. multinationals require employees to execute an employment agreement, they would face some risk by relying on the "performance-of-contract" derogation to legitimize cross-border data transfers to a global HRIS located in the U.S. To begin with, EU data protection authorities construe the derogations narrowly. In the case of the "performance-of-contract" derogation, the regulators likely would scrutinize whether the transfer to the third-party parent corporation is "necessary" for the performance of the contract between

the EU resident and the EU employer-subsidiary. This is because employees' personal data stored in a global HRIS often is used to perform functions that are in the interest of the parent corporation, such as succession planning, but have limited, if any, significance for the contractual relationship between the EU employee and the EU employer-subsidiary.

Other Issues

Service Providers

As previously noted, many U.S. multinational employers rely on third-party service providers to support global operations. Under the now-invalidated Safe Harbor, the employer could transfer EU personal data to these service providers if they themselves were certified to the Safe Harbor. In addition, EU-based managers and human resources personnel could rely on the service provider's Safe Harbor certification to enter data about EU employees directly into databases maintained by the service provider. The ECJ's decision has effectively eliminated this option.

With no Safe Harbor currently in place, U.S. multinational employers likely will need to rely on data transfer agreements to legitimize the transfer of EU personal data to U.S.-based service providers. The EU Commission has approved Standard Contractual Clauses for transfers of personal data between data controllers, *i.e.,* employers, and data processors, *i.e.,* service providers. As a practical matter, these employers should expect that their service providers will be inundated with requests to execute SCCs in light of the ECJ's decision. Consequently, there may be some delay getting these data transfer agreements in place.

Additional Guidance May Be Forthcoming

The invalidation of the Safe Harbor is a radical structural change to the relationship between the EU and the U.S. insofar as cross-border data transfers are concerned. With this change having an impact on more than 4,000 U.S. and EU businesses, the Commerce Department and EU data protection regulators will be under pressure to issue guidance on the implications of the ECJ's decision for companies that relied on the now-invalidated Safe Harbor.

Summary of Recommendations

In light of the ECJ's decision invalidating the Safe Harbor Framework, U.S. multinational employers should consider taking the following steps:

1. Watch for guidance issued by U.S. and/or EU regulators;
2. Monitor the progress of negotiations over a replacement Safe Harbor;
3. Evaluate Standard Contractual Clauses, Binding Corporate Rules, and the derogations as alternatives to the now-invalidated Safe Harbor Framework;
4. Consider using consent as a mechanism to legitimize cross-border transfers of applicants' personal data; and
5. Evaluate whether it is necessary to implement SCCs with any service providers.