Client Alert

pillsbury

Privacy, Data Security & Information Use

October 7, 2015

With Safe Harbor now "Invalid," Companies Must Change Data Practices

By Rafi Azim-Khan, Mercedes K. Tunstall, Steven P. Farmer, Andrew L. Caplan and Kelley D. Bledsoe

Europe's top court ruled that U.S. companies relying upon the "Safe Harbor Framework" data sharing regime to maintain information regarding EU citizens is "invalid." This means that any company relying upon the Safe Harbor Framework, and any U.S. company holding EU citizen data in the U.S., urgently needs to review and reform how such data is transferred and stored to avoid the risk of fines. Status quo is not an option.

Yesterday, the Court of Justice of the European Union (the "CJEU") delivered a striking blow to the fifteen-year-old regime governing EU-U.S. data transfers. Specifically, the CJEU declared invalid the safe harbour framework (the "Safe Harbor Framework" or the "Framework") that thousands of U.S. companies have relied upon to facilitate data transfers from the EU to the United States.

The CJEU's rationale for striking down the Safe Harbor Framework was primarily based upon their assessment that U.S. authorities have the ability to access personal data transferred from EU member states ("Member States") and process it in a way that is "incompatible…with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security." The CJEU's conclusion was largely informed by the 2013 revelations of Edward Snowden regarding the U.S. government's capture of personal data through the PRISM program.

This means that companies that have relied upon the Framework must look back to default EU standards from 1995 to determine whether their data sharing practices are permissible. Further, the CJEU's opinion has clarified the role of individual EU member states in enforcing these requirements.

In this client alert, we provide a brief discussion of the legal background that established the Safe Harbor Framework; the CJEU's analysis behind its decision; and practical steps companies can take to help ensure compliance.

Background on the Legal Framework Surrounding the Safe Harbor Framework

On October 24, 1995, the European Parliament and Council issued Directive 95/46, establishing that transfer of personal data from the EU to another country must meet EU standards or else cannot be transferred.[1] The rationale for this approach "is to protect the fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention"),…and in general principles of Community Law."[2]

As such, pursuant to Article 25(4) of Directive 95/46, if a country's privacy laws do not meet EU standards and ensure an adequate level of protection, EU Member States must prevent the transfer of data to the country in question.

However, the next section of Directive 95/46, Article 25(6), provides a mechanism by which the European Commission may find that a particular country does provide an adequate level of protection, by reason of its domestic law or international commitments, for the protection of the private lives and basic freedoms and rights of individuals, in accordance with the Directive.

Pursuant to this authority under Article 25(6) of Directive 95/46, the European Commission issued Commission Decision 2000/520 on July 26, 2000, which established the Safe Harbor Framework for data transfers between the EU and U.S. This Commission Decision states that U.S. companies subject to Federal Trade Commission or Department of Transportation jurisdiction may satisfy the requisite standard of "adequate" personal data protection by complying with Commission Decision 2000/520.[3] Until yesterday, companies in the U.S. storing, processing or transferring data from EU citizens were able to use this Safe Harbor Framework through an annual self-certification with the U.S. Department of Commerce.

The CJEU's Decision to Invalidate the Safe Harbor Framework

On June 25, 2013, Maximillian Schrems, an Austrian citizen, lodged a complaint with Ireland's Data Protection Commissioner (*Schrems v. Data Protection Commissioner*), claiming that his personal data was not protected when it was transferred to and stored in the U.S., from Ireland, by Facebook.[4] The Irish Data Commissioner dismissed the claim as inconsistent with the European Commission Decision 2000/520, which established the Safe Harbor Framework. Schrems then appealed his complaint to the Irish High Court, which requested an advisory opinion from the CJEU Advocate General on the following two questions:

1. In the course of determining a complaint made to the Commissioner that personal data is being transferred to another, non-EU country (in this case, the U.S.), the laws and practices of which are allegedly inadequate to protect the data subject, is the Commissioner absolutely bound by a Community finding to the contrary (here, Decision 2000/520), which also addresses Articles of the

[1] Council Directive 95/46, art. 25, §1, 1995 O.J. (L 281).

[2] *Id*. at pmbl. § 10.

[3] The seven core privacy principals included in the Safe Harbor Framework include: (1) **Notice**: organizations must notify individuals about the purposes for which they collect and use information about them; (2) **Choice**: organizations must give individuals the opportunity to choose (opt out) of third party information sharing—in the case of sensitive information, organizations must provide individuals the opportunity to affirmatively opt in to third party information sharing; (3) **Onward Transfer**: to disclose information to a third party, organizations must require the third party to comply with these Notice and Choice principles; (4) **Access**: individuals must have access to personal information about them, except where the burden or expense of providing access is disproportionate to the risks of individual privacy, or where the rights of persons other than the individual would be violated; (5) **Security**: organizations must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration and destruction; (6) **Data Integrity**: organizations must insure the integrity of personal information; and (7) **Enforcement**: this includes both private and government-level enforcement mechanisms to ensure compliance.

[4] Case C-362/14, *Schrems v. Data Prot. Comm'r* (Sept. 23, 2015) (opinion of AG Bot).

> EU Charter of Fundamental Rights, the provisions of Article 25(6) of Directive 95/46 notwithstanding?
>
> 2. Alternatively, may and/or must the Commissioner conduct his or her own investigation of the matter raised in the complaint, in light of factual developments that have occurred since the Community finding (Decision 2000/520) was first published?[5]

The High Court noted that Schrems, by the content of his complaint, actually alleged that the prevalence of mass data surveillance in the U.S. had rendered U.S. data protection practices inadequate under Decision 2000/520, thus calling to question the appropriateness of the Safe Harbor Framework itself.[6]

The CJEU Advocate General Yves Bot, on September 23, subsequently issued an opinion recommending that Decision 2000/520 (establishing the Safe Harbor Framework) be declared invalid (even though the Irish High Court, itself, did not submit that issue for express consideration).

In essence, Advocate General Bot argued that when personal data is transferred to the U.S., government agencies like the National Security Administration and Federal Bureau of Investigation are able to access the data *en masse*, without any targeted interception of communications or particular purpose. According to Bot, individuals have no ability to challenge such access, especially given that much of U.S. government access is carried out in secret and notice is not given to individuals that their data may be so accessed.[7] Although the Safe Harbor Framework allows access to data for purposes of national security, Bot argued that the Safe Harbor Framework does not provide protections consistent with legal process, or ensure that the U.S. government has a particular purpose for accessing the data.[8] Thus, according to Advocate General Bot, the rights to privacy and protection of personal data under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union are violated.[9]

Similarly, the CJEU held that even if the European Commission has adopted a decision pursuant to Section 25(6) of Directive 95/46 (*e.g.*, the Safe Harbor Framework), the EU national supervisory authorities, when hearing a claim concerning a person's rights and freedoms in regard to the processing of personal data, must be able to examine with "competent independence, whether the transfer of that data complies with requirements laid down by that directive."[10] In other words, according to the CJEU, Ireland's data protection authority would have the power to analyse specific claims under the existing Safe Harbor Framework. However, the CJEU recognised that such local authorities lacked the ability to adopt measures "contrary to" the Safe Harbor Framework.[11]

So, the CJEU then removed that limitation by invalidating the Safe Harbor Framework itself. Although the CJEU acknowledges that Directive 95/46 does not include an express definition for the term "adequate," and further, that "adequate" does not mean "identical" to EU privacy standards, the CJEU adopted Advocate General Bot's position that:

> The term "adequate level of protection" must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of

[5] *See id.* at ¶ 47.
[6] *See id.* at ¶¶ 42-43.
[7] See id. at ¶¶ 172-73.
[8] *See id.* at ¶¶ 163-66.
[9] *Id.* at ¶ 181.
[10] Case C-362/14, *Schrems v. Data Prot. Comm'r* ¶ 66 (Oct. 6, 2015).
[11] *See id.* at ¶ 52.

> fundamental freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of Directive 95/46 read in light of the [European] Charter (emphasis added).[12]

The CJEU notes that even after the Commission has adopted a decision that a particular country's privacy protections are "*essentially equivalent*" to those of the EU, and thus adequate, the Commission must periodically review whether that country's adequacy finding is still factually and legally justified.[13]

Applying this standard to the Safe Harbor Framework, the CJEU found that it deprives European citizens of fundamental rights, without providing corresponding legal process. The CJEU decision specifically notes that the Framework includes a mechanism by which:

> the applicability of safe harbour principles may be limited to meet national security, public interest, or law enforcement requirements, or by statute, government regulation or case law that provide conflicting obligations, provided an organization can demonstrate that its non-compliance with the Safe Harbor Framework is "limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization."[14]

The CJEU argues that these types of "exemptions" to the Safe Harbor Framework—without corresponding means of administrative or judicial redress—interfere with fundamental rights of EU citizens.

Perhaps most pointedly, the CJEU decision echoes the criticisms of Max Schrems and General Advocate Bot, and notes:

> Legislation is not limited to what is strictly necessary where it authorizes, on a generalized basis, storage of all the personal data of all persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail…[15]

The Road Ahead

With the Safe Harbor Framework being invalidated, EU domestic authorities may now decide for themselves whether the U.S. has "adequate" data protection measures under Directive 95/46. While it is possible that European domestic authorities could decide the U.S. has "adequate" privacy protections, it seems unlikely in light of the PRISM program. Although, perhaps with the U.S. government winding down its mass surveillance programs,[16] European privacy regulators could look differently upon U.S. privacy laws going forward.

In the meantime, however, the CJEU has determined U.S. privacy laws to be inadequate, and so companies holding, processing or transferring EU citizen data in the U.S. that relied upon the Safe Harbor Framework, must instead look to Directive 95/46, to find another way to transfer data from the EU to the U.S.

The one bright light for U.S. companies is that many may have already recognised that the Safe Harbor Framework had its days numbered because of an impending EU data regulation that is stricter and provides for larger fines (e.g., 2-5 percent of global revenue).

[12] *See id.* at ¶ 73.
[13] *See id.* at ¶ 76.
[14] *See id.* at ¶ 84.
[15] *See id.* at ¶ 93.
[16] USA Freedom Act, 50 U.S.C. § 1801 (2015).

Many companies have turned to Binding Corporate Rules ("BCRs") as a preferred alternative to the Safe Harbor Framework for those who have a lot of data flowing internationally. In essence, companies who have BCRs commit to certain data security and privacy standards relating to their processing activities. Once approved by the local data protection authority, the "blessed" scheme allows a safe environment within which multiple transfers can take place.

BCRs also have material long-term benefits in the sense that some upfront work, via preparing and submitting the application, should reduce risk of fines and undoubtedly position an applicant in line for a privacy "seal" once the new EU Regulation is introduced.

Model contract clauses, which can also be used to "adequately safeguard" data transfers from Europe, are also an alternative route to ensuring compliance, and can work for certain companies. However, they do have a number of drawbacks compared to BCRs (inflexibility, often large numbers of contracts being required, a need to update regularly and so on).

In short, any company that stores, processes or transfers EU citizen data in the U.S., whether large tech giants/big brands or smaller enterprises, must urgently address their procedures, policies and documents regarding how they handle data. Alternative arrangements to the Safe Harbor Framework must be adopted quickly.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Rafi Azim-Khan (bio)
London
+44.20.7847.9519
rafi@pillsburylaw.com

Mercedes K. Tunstall (bio)
Washington, DC
+1.202.663.8118
mercedes.tunstall@pillsburylaw.com

Steven P. Farmer (bio)
London
+44.20.7847.9526
steven.farmer@pillsburylaw.com

Andrew L. Caplan (bio)
Washington, DC
+1.202.663.8110
andrew.caplan@pillsburylaw.com

Kelley D. Bledsoe (bio)
Washington, DC
+1.202.663.8803
kelley.bledsoe@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.