BAKER & MCKENZIE

LEGALBytes

Global Information Technology & Communications Industry & Practice Group

Special Edition

October 2015

Print Version

What did the Judgment decide regarding the US/EU Safe Harbor Program?

What question was the CJEU asked to resolve?

What key concerns was the Judgment based on?

What does the Judgment mean for European data protection?

As a matter of US law, is the US/EU Safe Harbor Program still operational?

What Happens Now?

What should US companies participating in Safe Harbor do now?

What does the Judgment mean for European trading partners of Safe Harbor certified companies?

Now that the CJEU has issued its Judgment, are all of these issues settled?

Where can I go to get source information?

For more information, please contact:

North America

Brian Hengesbaugh
Partner, Chicago

Frequently Asked Questions on the Judgment of the CJEU on the US/EU Safe Harbor Program

What did the Judgment decide regarding the US/EU Safe Harbor Program?

The Court of Justice of the European Union ("CJEU"), following the opinion of the Advocate General, invalidated European Commission Decision 2000/520 dated July 27, 2000 ("Decision"), which allowed transfers of personal data to US companies that self-certified under the US/EU Safe Harbor Program ("Safe Harbor").

The comparable Swiss program, called the "US/Swiss Safe Harbor program," is not formally affected by the CJEU's Judgment, as Switzerland is not a member of the EU. However, it is likely to be put in question from a Swiss law perspective given the similarities with the US/EU Safe Harbor Program.

What question was the CJEU asked to resolve?

The CJEU was asked to consider whether the Irish Data Protection Commissioner "may and/or must" independently evaluate whether the third country (in this case, the United States through the implementation of Safe Harbor) offers "adequate protection" for personal data within the meaning of the European Data Protection Directive (95/46/EC) ("Directive"), or whether the Irish Data Protection Commissioner is bound by the Decision, as issued by the European Commission ("EC") under Article 25(6). The concerns in the underlying case related to the extent of data accessed by the US National Security Agency and other US authorities as described in Edward Snowden's revelations in 2013.

What key concerns was the Judgment based on?

The Judgment focuses on the issue of whether the Decision "ensures" an "adequate" level of protection of personal data. The Court found – based on a "strict" review - that the EC's decision does not provide for an "adequate" level of protection (i.e., a level of protection that is "essentially equivalent" to that guaranteed in the European Union), because (i) it provides for a general and unlimited derogation from the Safe Harbor principles where national security, public interest, or law enforcement requirements are concerned, and (ii) does not "refer to the existence of effective

+1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Lothar Determann
Partner, Palo Alto
+44 20 7919 1914
lothar.determann@bakermckenzie.com

Harry Valetk
Of Counsel, New York
+1 212 626 4285
harry.valetk@bakermckenzie.com

Amy de La Lama
Of Counsel, Chicago
+1 312 861 2923
amy.delalama@bakermckenzie.com

EMEA

Dyann Heward-Mills
Partner, London
+44 20 7919 1269
dyann.heward-mills@bakermckenzie.com

Denise Lebeau-Marianna
Partner, Paris
+33 1 4417 5333
denise.lebeau-marianna@bakermckenzie.com

Raffaele Giarda
Partner, Rome
+39 06 4406 3224
raffaele.giarda@bakermckenzie.com

Francesca Gaudino
Partner, Milan
+39 0 2762 31452
francesca.gaudino@bakermckenzie.com

Nicolas Passadelis
Partner, Zurich
+41 443 841 209
nicolas.passadelis@bakermckenzie.com

Matthias Scholz
Partner, Frankfurt
+49 69 299 08180
matthias.scholz@bakermckenzie.com

Julia Wendler
Partner, Munich
+49 89 552 38242
julia.wendler@bakermckenzie.com

Wouter Seinen
Partner, Amsterdam
+31 20 551 7161
wouter.seinen@bakermckenzie.com

Elisabeth Dehareng
Partner, Brussels
+322 639 3705
elisabeth.dehareng@bakermckenzie.com

legal protection" against interference of US State entities with the fundamental rights of the persons whose data is transferred from the European Union.

Focusing on the EC's failure to state, in its Decision, that the United States in fact "ensures" an adequate level of protection by reason of its domestic law and its international commitment, the Court did not address nor analyze the many changes in US law and policy that have occurred since those revelations came to light, as noted in our previous FAQs on the opinion of the Advocate General.

The CJEU also did not consider or acknowledge that European intelligence services and law enforcement authorities operate similar programs and cooperate closely with their US allies. The Irish court which referred the matter to the CJEU did acknowledge these facts, which seem particularly relevant to the question what is "adequate" - a relative concept that should be viewed in comparison with practices in the EEA Member States.

What does the Judgment mean for European data protection?

The Judgment eliminates an important mechanism that EU companies had used for fifteen years to transfer personal data to participating US companies. It also removes the benefit for US companies to participate in the program, which requires them to submit to the authority of US Federal Trade Commission (FTC) for the enforcement of the Safe Harbor rules. Regardless of any perceived shortcomings in Safe Harbor enforcement, the reality is that the FTC has pursued dozens of Safe Harbor cases to conclusion, and US companies were greatly motivated by concerns about FTC enforcement actions. This FTC enforcement role for European data protection rights in the US will end, unless the negotiations for a revised Safe Harbor program ("Safe Harbor 2.0") are completed and the agreed framework is subsequently approved internally.

The Judgment as written also calls into question the validity of European Commission decisions of adequacy for other countries and systems, or at a minimum invites Member State data protection authorities and/or the courts in Member States to second guess the validity of those decisions. If this approach is followed, the validity of alternative means of trans-border data flows such as standard contractual clauses (so-called "Model Contracts") and binding corporate rules may be revisited, with potential negative consequences for companies in the Common Market, European unity and legal harmonization.

As a matter of US law, is the US/EU Safe Harbor Program still operational?

Yes. The US Department of Commerce continues at present to maintain the Safe Harbor program, including the website with the list of participating companies. Likewise, the Federal Trade Commission's authority to pursue violations of the promises to adhere to the Safe Harbor Privacy Principles remains unaffected. Companies would need to de-certify from the Department of Commerce list, and remove all references to Safe Harbor in privacy statements and other materials, in order to exit the

Raul Rubio
Partner, Madrid
+34 91 436 6639
raul.rubio@bakermckenzie.com

Asia Pacific

Anne-Marie Allgrove
Partner, Sydney
+61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Anna Gamvros
Partner, Hong Kong
+85 2 2846 2137
anna.gamvros@bakermckenzie.com

Ken Chia
Partner, Singapore
+65 643 42558
ken.chia@bakermckenzie.com

Yee Chung Seck
Partner, Ho Chi Minh City
+848 352 02633
yeechung.seck@bakermckenzie.com

Daisuke Tatsuno
Partner, Tokyo
+81 3 6271 9479
daisuke.tatsuno@bakermckenzie.com

Latin America

Carolina Pardo
Partner, Bogota
+571 634 1559
carolina.pardo@bakermckenzie.com

Guillermo Cervio
Partner, Buenos Aires
+54 11 431 0223
guillermo@bakermckenzie.com

Flavia Rebello
Partner, Sao Paulo
+55 11 3048 6851
flavia.rebello@trenchrossi.com

Sergio Legorreta-Gonzalez
Partner, Mexico
+52 555 279 2954
sergio.legorreta-gonzalez@bakermckenzie.com

program. The promises made during the time of the company's participation in Safe Harbor would continue to apply. Companies should examine decisions about whether to de-certify carefully in light of the company's risk profile and specific circumstances.

What Happens Now?

To avoid a patchwork of potentially contradicting decisions by the Member State data protection authorities, the European Commission is expected to publish, together with the data protection authorities of the Member States, further analysis and guidance in the coming weeks for companies trying to address the implications of the Judgment. Such guidance should facilitate a coordinated response from the Member State data protection authorities, and would be an appropriate vehicle to define a formal transition period, if any will be offered.

Although it has given no particular timetable, the EC has indicated its intent to continue working with US authorities to reach agreement on Safe Harbor 2.0 after nearly two years of negotiations. Such an amended program should be framed in a manner that addresses the concerns in the CJEU Judgment, although the EC would need to conduct internal consultations within the EU before issuing, and may have to allow more discretion and residual sovereignty of national data protection authorities. Ultimately, like other decisions, it could be challenged judicially.

In response to the Judgment, EC Commissioner Věra Jourová made a point that companies must apply other cross-border transfer mechanisms in light of the Judgment. An additional thread in this discussion of which companies should be aware of is the impending finalization of the European Data Protection Regulation, which the Commission stated should be complete by the end of this year. Click here for an article that summarizes the draft EC Regulation.

What should US companies participating in Safe Harbor do now?

There is no one-size-fits-all solution to these issues, as companies may have different risk profiles, tolerance, and other factors that may affect their approach to this issue. In general, US companies participating in Safe Harbor should take steps to assess the situation and determine the best course of action in the short term and long term. Three steps all such companies should consider right now are:

1. Take inventory of reliance on Safe Harbor. Take inventory of the scope of the company's reliance on Safe Harbor, including: (i) whether it has local subsidiaries or other operations in the EU that rely on its Safe Harbor; (ii) from what countries it receives personal data under Safe Harbor; (iii) which categories of data are covered (e.g., employee data, customer data, health data, or other); (iv) where the company has made promises related to Safe Harbor (e.g., in employee notices, website privacy policies, customer contracts, EU subsidiary registrations with authorities, and the like); and (v) what particular risk factors may make enforcement actions or individual data subject complaints more likely (e.g.,

challenging works councils/employee representatives, prior experience with complaints, or the like). The inventory should also account for any legacy solutions already in place, such as supplemental Model Contracts for certain jurisdictions or consents.

2. Consider potential short-term solutions and whether to de-certify from Safe Harbor. Determine whether the company could implement certain solutions on a short term basis, such as the implementation of Model Contracts or consent or other derogations. Note that implementation of short-term solutions may, depending on the jurisdiction, attract duties to update registrations with authorities, to consult with works councils or data protection officers, to update notices or privacy policies, or take other steps. Also, there may be risks with certain solutions, such as consent, depending on the context (e.g., data protection authorities may not consider employee consent to be valid in all countries because of concerns that it is not freely given). Depending on how far the company makes it with respect to implementing the short-term solution, and the overall context of its program and risk profile, the company should consider whether to de-certify from Safe Harbor and remove all privacy statements about Safe Harbor in light of the risks from an US and EU standpoint.

3. Consider whether to enhance the company's global privacy program over the longer term. The company should consider whether to adopt binding corporate rules (BCRs) or other solutions that may take some time to implement (e.g., currently 12 to 18 months depending on the authorities and complexity of the case) but nevertheless may provide a broader solution over the longer term. In this regard, the company may also wish to consider seal programs or other codes of conduct that may become available under the EC Regulation, and/or participation in Safe Harbor 2.0 if that becomes available.

What does the Judgment mean for European trading partners of Safe Harbor certified companies?

European companies who have been doing business with participants in the Safe Harbor will now have to revisit their compliance obligations and options, which could disrupt their data protection compliance programs and established business relationships. They may have to ask their US counterparties to consider Model Contracts, binding corporate rules (among members of multinational groups of companies) or other approaches, which would have an impact also in terms of cost, time for implementation and administrative burdens. European companies may have to update their filings with data protection authorities as well as all information notices (e.g., privacy policies, IT policies, removal of Safe Harbor references). Also, European companies may become subject to approval requirements with local data protection authorities for data transfers to the US.

Now that the CJEU has issued its Judgment, are all of these issues settled?

No. There are many important developments yet to come. The EC has indicated over the next few weeks it will work Member State data protection authorities regarding a consistent approach to the

issues. The EC and the US Department of Commerce may take steps to announce part or all of Safe Harbor 2.0. The EC will continue to press through the "*Trilogue*" process to complete the EC Regulation, reportedly this calendar year. And, the Member State data protection authorities may act individually or, through the Article 29 Working Party, to identify guidance on how they will approach these issues. It will thus be important to track carefully any updates or guidance in the coming weeks.

Where can I go to get source information?

Source	**Latest**	**Key point**	**Watch this space**
CJEU	Press release (6 October 2015) Judgment (6 October 2015)	Safe Harbor invalid	CJEU press release page
European Commission	Statement (6 October 2015)	Commission to issue guidance on the ruling but no time frame offered. Aim is to step up discussions with the US towards a renewed and safe framework for the transfer of personal data across the Atlantic. In the meantime, organizations to rely on alternative mechanisms to legitimize transfers to the US (model clauses, BCRs, derogations, consent)	Commission press release page Commission daily news page
Article 29 Working Party	Press release (6 October 2015)	A first round of discussions between experts is organized week commencing 5 Oct. An extraordinary plenary meeting of the Working Party will be shortly scheduled.	Article 29 Working Party press release page