ALSTON & BIRD

Schrems ECJ / Safe Harbor Ruling – FAQs

The European Court of Justice (ECJ) ruled on October 6, 2015, that the Safe Harbor framework for the transfer of personally identifiable information (PII) from the European Economic Area (EEA) to the United States is invalid. This decision eliminated one of the mechanisms available to companies for the transfer of PII to the United States in accordance with EEA data protection laws. The following Frequently Asked Questions (FAQs) discuss the practical impact of the ECJ decision and alternative mechanisms to enable the continued flow of PII within organizations and to service providers.*

Safe Harbor Ruling FAQs

* Please note that events are moving very quickly in Europe and the United States and that new developments may necessitate updates to these FAQs in order to maintain their currency. These FAQs were authored on 15 October 2015.

ALSTON & BIRD

Schrems ECJ / Safe Harbor Ruling – FAQs

1. What is Safe Harbor and why does it matter?

The "Safe Harbor" program is a framework developed by the U.S. Department of Commerce and the European Commission in 2000 for the transfer of PII. Alston & Bird's own Peter Swire was a member of the U.S. team that negotiated Safe Harbor.

European Union Directive 95/46/EC ("Directive"), enacted in 1995, required member countries of the European Union to put in place privacy laws that, among other things, prohibit the transfer of PII to countries outside the EEA that do not provide "adequate protection" for data privacy rights. The U.S. and EEA established Safe Harbor to address this issue.

By joining Safe Harbor, organizations publicly commit to protect the PII they process within the Safe Harbor principles. Safe Harbor participants also accept the jurisdiction of the U.S. Federal Trade Commission. Organizations that are Safe Harbor certified are deemed to meet the Directive's standards of adequacy for the protection of PII, thus enabling transfer of personal information from the EEA to the U.S.

Over 4,000 U.S. companies rely on Safe Harbor, taking advantage—until now—of the administrative simplicity of the framework by limiting the data transfer formalities associated with Model Clauses, binding corporate rules (BCRs) and other means of allowing data transfers between the EEA and the U.S.

2. What does the ECJ Safe Harbor ruling say?

The decision of the ECJ invalidated the Safe Harbor program due to a concern that, according to the ECJ, U.S. companies may be required to provide PII to U.S. national security agencies "on a generalized basis" and "without any differentiation, limitation or exception" without a sufficient means of redress for European individuals. Furthermore, the ECJ ruled that Safe Harbor unlawfully restricted European data protection authorities' (DPAs') powers (1) to investigate individuals' complaints related to claims of insufficient protection of their PII under Safe Harbor and (2) to suspend PII exports to the U.S.

3. My company was relying on Safe Harbor to transfer personal data from the EEA. What should I expect?

DPAs are well aware that the 4,000+ U.S. companies that currently rely on Safe Harbor will need sufficient time to address the ruling. National DPAs such as the UK DPA or the French DPA already have released public statements showing a rational reaction to the ruling. Likewise, EU Commissioner Vera Jourova stated that "it is important that transatlantic data flows can continue, as they are the backbone of our economy."

The Article 29 Working Party convened October 8 to deliberate on the ruling. A full plenary meeting is planned on Thursday, October 15, and it is expected that the Article 29 Working Party will publish a position on the ruling as well as specific guidance on possible alternatives for industry to transfer personal information outside the EEA. It is not expected that DPAs will start sanctioning companies, but companies will require a grace period to allow transitioning to other transfer options.

Jourova's statement and the European Commission's press release is available at: http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.

The French DPA's press release is available (in French) at: http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/.

The UK DPA's press release is available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/.

4. Do I need to stop transferring PII out of Europe?

The impact of the Safe Harbor decision depends upon what mechanism an organization uses to move PII out of Europe. If you use only Safe Harbor, then it is advisable to promptly evaluate other alternatives for PII transfer. We outline those alternatives below.

DPAs have signaled that immediate enforcement against Safe Harbor companies is not planned. See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/. But enforcement actions, while unlikely in the immediate term, are possible. Therefore it is prudent to move with deliberate speed to implement an alternative mechanism to establish adequate protection of privacy rights pursuant to EEA data protection laws.

5. Do I need to stop transferring PII to my vendors who are Safe Harbor participants?

It is important to take stock of your service provider relationships to determine which, if any, involve transfers of PII under Safe Harbor. In those cases, consider requiring service providers to sign the "Model Contract," discussed in more detail below. We understand some service providers are attempting to persuade customers to sign new contract terms that are not a part of the Model Contract and are more favorable to the service providers perhaps than existing contract terms. Take care not to sign any new terms in addition to the Model Contract without full review of those proposed additional terms.

If a service provider does not promptly agree to sign the Model Contract or to demonstrate another basis for the transfer under EEA data privacy law (such as a permit issued by a DPA), then we recommend assessing the need for further action to avoid a legal compliance issue.

6. I am a data controller under EEA law. What should I do?

Although we do not anticipate immediate enforcement actions, the Safe Harbor ruling has had an immediate result that Safe Harbor is invalidated and no longer constitutes a reliable basis to transfer personal information to the U.S.

Given the interim legal uncertainty, we recommend that you carry out an inventory of your organization's data streams to the U.S. under Safe Harbor. In addition, start thinking of a strategic plan to respond. Consider doing the following:

- Identify EEA-affiliated companies that transfer PII to the U.S. and relevant information systems containing EEA personal information.
- Identify third-party service providers that are Safe Harbor certified, such as cloud providers, information hosting companies, whistleblowing hotline providers and others.
- For each of the above, you may find valuable information in privacy impact assessments conducted earlier or in overviews compiled by your privacy department. Also, data privacy officers you retain in certain jurisdictions may have the information you are looking for.
- Establish a priority list of information systems that require immediate attention both for transfers between affiliated companies or to and from third-party service providers. This would be typically be risk based, after evaluating the amount of information affected or the sensitivity of information. For instance, a consumer database would likely be higher on the list than a corporate contact database.
- Locate and review service contracts with providers and assess workable alternatives. Ask your providers what alternatives they can offer to accommodate your concerns.

As soon as more formal DPA and European Commission guidance starts to become available, companies will need to re-assess and may need to amend their PII data transfer strategy with respect to EEA-U.S. PII streams. Strategic corrections will need to be reflected in policy documents, data processing contracts, notices and other internal and external facing documentation. Furthermore, DPA notifications will need to be amended to avoid questioning and potential DPA audits.

7. I am a data processor under EEA law whose clients rely on my Safe Harbor certification. What should I do?

You should work to understand your clients' concerns in light of the ECJ decision and develop options. For example, you should consider developing an alternative strategy for transfers of personal data that you can present to your clients. EEA DPAs have promised to issue guidance on how to secure existing Safe Harbor data transfers, and your approach should incorporate this guidance.

Do not forget to focus on your subcontractors/vendors that receive your clients' PII. Your clients will expect you to have a strategy ready to allow these to have access or receive PII in line with applicable adequacy restrictions. Consider reaching out to subcontractors/vendors and involve them in your offerings towards your clients.

In some circumstances, you may better address your clients' concerns by limiting the data you handle to non-PII, such as anonymized or irreversibly key-coded data.

8. Are there compliance alternatives to Safe Harbor for data transfers to the United States?

Yes. The Directive provides alternatives to Safe Harbor for the purpose of demonstrating the required "adequate level of protection" for transfers of PII from the EEA. We do not consider the Safe Harbor ruling to directly affect these alternatives to Safe Harbor, although there is some future risk based on a technical analysis of the ECJ decision.

Compliance alternatives include:

- Model Clause contracts (Model Contracts).
- Binding corporate rules (BCRs).
- A permit issued by each applicable DPA for the transfers of PII in question.
- The "unambiguous consent" of individuals.
- An exception such as the need to transfer information in light of the performance of a contract, a public interest or legal necessity.

Each of these alternatives carries certain requirements and is subject to certain limitations.

9. What are Model Contracts and how are they used?

Model Contracts (also sometimes called "Model Clauses" or "Standard Clauses") are sets of standardized provisions approved by the European Commission that can be used to authorize transfers of PII from any EEA member state to any recipient outside of the EEA.

A Model Contract is a template agreement containing minimum contractual clauses to protect PII transferred between an EEA-based data exporter and a data importer outside of the EEA. A set of Model Contracts is available for both controller to controller (C2C) and controller to processor (C2P) data transfers. Importantly, the exporter in Europe must be a data controller. Data processors are not authorized to export data on the basis of a Model Contract.

10. What are BCRs and how are they used?

Binding Corporate Rules (BCRs) are a technique to transfer PII between affiliates of the same corporate group of companies. BCRs take the form of an overarching policy or code of conduct that stipulates core principles of data protection and are negotiated with the DPAs.

As part of the BCR process, a "lead" DPA will review the BCR materials and engage in subsequent consultations with other DPAs. Because BCRs involve the approval of local DPAs, BCRs create a strong regulatory presumption that the approved organization has an adequate level of protection for personal data. Based on current rules, local DPAs cannot directly overturn a finding of adequacy based on BCRs.

BCRs require an upfront investment, and the typical approval process can take 12–18 months. However, once in place, BCRs simplify compliance with EEA privacy law for projects involving the cross-border transfer of PII among affiliated companies. This increases efficiency in reviewing, designing and implementing any projects that involve PII from EEA data subjects.

11. How and when is it a good idea to obtain "unambiguous consent" of EEA data subjects?

Unambiguous consent may be a workable solution in certain circumstances, but impractical in others. Consent offers a compliance alternative to Safe Harbor where only limited transfers occur and the likelihood that an individual would want to revoke his/her consent appears limited.

In practice, however, not every data transfer situation is appropriate for consent. For example, the Article 29 Working Party has held that data subject consent should not be used for data transfers involving repetitive and bulk streams of data. In addition, data subject consent often does not work in the employment context as consent from employees is not generally considered freely given.

This said, consent may prove a viable option for companies with a strong Internet presence, including search engines, social networks or even online merchants. In the Internet context, a consent button should be technically easy to implement and provides reliable evidence of consent.

12. Does the Safe Harbor ruling affect transfers of data for human resources purposes?

Yes. The ECJ ruling directly affects any transfers of PII, including HR data, from the EEA that relied upon a Safe Harbor certification. This includes transfers of PII for human resources purposes within a particular company or corporate group.

13. Does the Safe Harbor ruling affect transfers of data for litigation / e-discovery purposes?

Yes. The Safe Harbor ruling directly affects transfers of PII for litigation or e-discovery purposes, even if discovery or production is compelled under applicable law. After the Safe Harbor ruling, the Safe Harbor certification is no longer an officially recognized, reliable basis for ensuring the required "adequate level of protection" for litigation or e-discovery related transfers of PII from the EEA to the U.S. We recommend developing an alternative strategy for data transfers based on your specific situation.

You may be able to rely on an exception within EEA data privacy law that allows for the transfer of the data when the transfer is necessary for the exercise or defense of a legal claim. Such a possibility is especially relevant for specific transfers during ongoing judicial proceedings. For instance, if you would need to access the emails of a specific employee located in the EEA upon being served with a subpoena, strong arguments can be made that you can rely on the exception of legal necessity. In such a scenario, compliance with other EEA requirements, such as registration with the DPA and information of individuals, will be critical. The analysis of litigation and e-discovery issues is very fact-intensive and should be conducted on a case by case basis.

Schrems ECJ / Safe Harbor Ruling – FAQs

14. Does the Safe Harbor ruling affect transfers of data to countries other than the United States?

No. The ECJ decision impacts only transfers of PII from the EEA to the United States under Safe Harbor. European law requires establishing adequate protection for transfers of PII to all but a small handful of other countries. But the options for establishing adequacy were not impacted by this decision.

If you have any questions or would like additional information, please contact one of the following:

James A. Harvey
jim.harvey@alston.com
404.881.7328

David C. Keating
david.keating@alston.com
404.881.7355

Jan Dhont
jan.dhont@alston.com
+32 2 550 3709

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com