Navigating the European Court of Justice’s data protection ruling
What is the Safe Harbor Framework?

Under the Data Protection Directive from the European Union (EU), personal data (essentially any information about individual persons) cannot be transferred outside of the EU to any jurisdiction that EU authorities have not found to provide an adequate level of data protection according to EU standards, unless there are appropriate measures in place to legitimize the transfer. Under these requirements, the United States has not been deemed to have a comprehensive data protection law and thus has not been considered an “adequate” jurisdiction. In 2000, the EU and the US negotiated a special arrangement – the Safe Harbor Framework – under which most US businesses could publicly certify that they adhere to privacy principles considered adequate by EU standards, subjecting themselves to enforcement action by the US Government if they should be found to fail to do so. Businesses with Safe Harbor certification could then receive personal data from the EU to the same extent as businesses in “adequate” jurisdictions.

What happened?

On 6 October 2015, the European Court of Justice (ECJ) declared the US Safe Harbor agreement as invalid largely because it does not protect data transferred from the EU to the US from being accessed in bulk by US intelligence agencies. The ECJ decision also establishes an individual's right to challenge any similar data-sharing agreements through their national data protection authorities (DPAs).

What is the impact of the decision?

The full impact is unclear, but we do know that Safe Harbor is changing, and those analyzing the implications of the ruling are indicating that it likely cannot be relied on as it is today. The ruling is another indication that legitimizing cross-border transfer will be a prominent topic for both the EU DPAs and the US Government. As such, this is a good opportunity for companies to reevaluate their current mechanisms for transferring EU personal data across their operations in a secure and compliant manner.

What are your options?

Safe Harbor in its current form was not the only mechanism under which personal data may be transferred to a “non-adequate” jurisdiction. Alternatives include:

- Standard contractual clauses issued by EU regulators, called model clauses, can be put in place by the sending and receiving parties to cover the data in question.
- Multinational organizations can adopt binding corporate rules (BCRs) governing data transfer and have these approved pursuant to EU regulations.
- Consent of the data subjects (the people whose data is being transferred) can be obtained.

Given the rapidly changing regulatory requirements, businesses receiving EU-source personal data in the US will now need to determine what changes are required to comply with EU regulations, absent the Safe Harbor. When evaluating which alternative solution to implement, companies should consider which of the mechanisms best meet their operational needs and limitations. For example, BCRs have many operational benefits but require a level of privacy program maturity that may take a while to achieve. Obtaining consent from data subjects can be logistically challenging and unrealistic for large corporations. Additionally, on the employee side, consent may not be considered as freely given due to the employer-employee relationship and therefore complicate the legitimacy of that mechanism. Using model clauses may be more practical in the short term, but they include requirements and liabilities that were not part of the Safe Harbor program and can be difficult to apply.
Are you prepared?

Although the full impact of the decision has yet to be determined, companies can do a number of things to prepare. The list below represents, at a high level, the questions companies should ask themselves before transferring personal data outside of the EU.

| Understand the flow of EU personal data | ▪ Do you know what entities in the EU are transferring personal data out of the region and what entities receive it?  
▪ Do you know where the EU personal data is across your enterprise, including when service providers process it?  
▪ Do you know whether EU sensitive personal data is transferred and for what purposes? |
| Understand the use of EU personal data | ▪ Do you provide notice at the time EU personal data is collected?  
▪ Are you confident that EU personal data is used only for the purposes for which it was collected?  
▪ Do you have controls in place to limit access to EU personal data based on legitimate business needs?  
▪ Do you have an effective process in place to address complaints and access requests from data subjects?  
▪ Do you have a process in place to address incidents involving personal data?  
▪ Do your contracts with service providers include the necessary obligations to protect EU personal data for privacy and security? |
| Understand the governance over EU personal data | ▪ Have you identified and addressed each of the specific requirements of the cross-border transfer mechanism you decided to adopt?  
▪ Have you published policies, procedures and guidelines to guide the use of EU personal data?  
▪ Have you trained your employees on the appropriate use of EU personal data?  
▪ Are you monitoring compliance with your privacy obligations and addressing gaps?  
▪ Have you established roles to manage the privacy and security of the EU personal data that you process? |
EY can help

EY has professionals ready to provide privacy risk and compliance services to help clients evolve their privacy programs to address new regulatory requirements. EY brings years of experience developing privacy programs for Fortune 100® and Fortune 500® companies. We assist global companies by developing programs that include practical cross-border transfer solutions that meet the regulatory requirements of various countries, including the EU. We helped companies across various industries effectively adopt model clauses and BCRs with the necessary policies, controls, monitoring and governance that these regulatory mechanisms merit.

EY can help you navigate the rapid changes in regulatory requirements by helping evaluate and improve your privacy program and data protection practices.

Our global network of privacy practitioners has proven experience in privacy governance, risk and compliance service offerings. EY privacy professionals collaborate with our European law practice, our security professionals and their Advanced Security Centers around the globe, and our Governance Risk and Compliance (GRC) systems professionals who work with our clients to harness the power of GRC technology to improve privacy management.

As we work with our clients to address the recent decision from the ECJ we focus on:

- **Enabling decision making.** We help companies determine what mechanism for legitimizing cross-border transfers from the EU appropriately addresses their needs and capabilities. In particular, we first determine whether an approach should be structured with permanence in mind, or as a step as the company builds toward BCR in parallel.

- **Implementation.** We track the EU personal data throughout its life cycle – from the time of collection, through use, internal sharing, disclosure and retention to its secure disposal. We design and implement a range of controls that allow the company to truly meet its compliance obligations while taking advantage of efficiencies that come with the implementation of technical controls over the data.

- **Monitoring.** We establish business processes and controls to assist the company in applying consistency to its obligations over the information it processes. Compliance is not a point-in-time exercise but a process that must withstand regular assessment and be adaptable for improvement and scalability.

- **Governance.** The governance over any set of complex compliance obligations has various facets. In the case of regional requirements that impact a company’s global transfers of data, the first aspects we address are roles and responsibilities that can effectively execute their respective tasks. Cross-border transfers also bring about questions about the company’s global footprint and compliance obligations from countries outside of the EU (limitations over the cross-border transfer of personal information exist in many countries worldwide). As we help clients design and implement strategies for meeting European requirements we weigh the impact of those approaches and alignment with our clients’ overall information management needs.

---

Contact us

Siobhan M. MacDermott
Principal
Ernst & Young LLP
+1 415 894 8285
siobhan.macdermott@ey.com

Sagi Leizerov, PhD
Executive Director
Ernst & Young LLP
+1 703 747 0899
sagi.leizerov@ey.com