What is Safe Harbor?
An agreement between the European and United States, invalidated by the Court of Justice of the European Union in 2015, that allowed for the legal transfer of personal data between the EU and U.S. in the absence of a comprehensive adequacy decision for the United States. It was replaced by the EU-U.S. Privacy Shield in 2016.

Historical Timeline

On 16 March 2016: Twenty-seven civil rights organizations declared that they do not believe that the Privacy Shield arrangement between the United States and the European Union complies with the standards set by the Court of Justice of the European Union (CJEU), including in the recent case invalidating the legal underpinnings of the Safe Harbor Framework. Without more substantial reforms to
ensure protection for fundamental rights of individuals on both sides of the Atlantic, the groups consider Privacy Shield to put users at risk, undermine trust in the digital economy, and perpetuate the human rights violations that are already occurring as a result of surveillance programs and other activities.

On 29 February 2016: European Commission issued the legal texts that will put in place the EU-U.S. Privacy Shield and a public a draft "adequacy decision" of the Commission (including the Privacy Shield Principles companies have to abide by, as well as written commitments by the U.S). Subsequently, Article 29 Working Party announced its intention to conduct an assessment of the corresponding documentation and to adopt a draft opinion at the next plenary meeting on 12 and 13 April 2016.

On 3 February 2016: Article 29 Working Party (WP29) welcomed the fact of the conclusion of the negotiations between the EU and the U.S. on the introduction of a "EU-U.S. Privacy Shield," which meets the deadline set by the WP29 in its statement of 16 October. It looks forward to receive the relevant documents in order to know precisely the content and the legal bindingness of the arrangement and to assess whether it can answer the wider concerns raised by Schrems judgment as regards international transfers of personal data.

On 2 February 2016: With some delay, the EU Commission announced an agreement with the U.S. on a new framework for transatlantic data flows called “EU-US Privacy Shield.” The new arrangement is built on the following elements: a) Strong obligations on companies handling Europeans' personal data and robust enforcement, b) Clear safeguards and transparency obligations on U.S. government access, c) Effective protection of EU citizens' rights with several redress possibilities (including an ombudsman).

On 28 January 2016: An amendment has been added to the Judicial Redress Act (JRA) which may lead to further disruptions in the U.S.-EU negotiations on an agreement to replace the Safe Harbor framework. The added language pertains to transfers of personal data for commercial purposes between certified foreign countries and the U.S., and adds requirements that the U.S. Attorney General certify that the foreign country’s “policies regarding the transfer of personal data for commercial purposes ... do not materially impede the national security interests of the United States.” National security/surveillance issues represented the reason for fundamental disagreements in the Safe Harbor negotiations so far, and the recent amendment is striking directly at that fissure.

On 25 January 2016: Electronic Privacy Information Center (EPIC) finally succeeded in forcing the U.S. Department of Justice (DOJ) to release the full text of the EU-U.S. Umbrella Agreement. EPIC sued the DOJ last year after the agency failed to act on EPIC's Freedom of Information Act request for the secret agreement. The Umbrella Agreement outlines data transfers between EU and U.S. law enforcement agencies and is the basis for the Judicial Redress Act currently before Congress. EPIC has criticized the legislation and recently urged the Senate to delay action on the bill until the DOJ releases the Umbrella Agreement and the Judiciary Committee holds a hearing on the legislation.

On 19 January 2016: the U.S. Chamber of Commerce, along with BUSINESSEUROPE, DIGITALEUROPE, and the Information Technology Industry Council issued a letter to President Obama, the presidents of the European Commission and Council, and the heads of the 28 European Union member states underlining the need to urgently reach an agreement on a new Safe Harbor data transfer mechanism as well as create long term certainty for businesses of all sizes that depend on the seamless flow of data and information across the Atlantic.
**On 6 November 2015**: EU Commission issued guidance on transatlantic data transfers and urged the swift establishment of a new framework following the ruling in the Schrems case. The Commission in its Communication stressed a) that the Safe Harbour arrangement can no longer serve as a legal basis for transfers of personal data to the U.S. b) the Commission will continue and finalise negotiations for a renewed and sound framework for transatlantic transfers of personal data, which must meet the requirements identified in the Court ruling and c) other adequacy decisions will need to be amended, to ensure that Data Protection Authorities remain free to investigate complaints by individuals.

**On 26 October 2015**: With particular regard to the CJEU decision in the Schrems case, Data Protection Authorities in Germany released a joint statement regarding transfers of personal data from EU to U.S. in general and Safe Harbor in particular. Besides highlighting the independence of Data Protection Authorities and abandoning Safe Harbor as valid mechanism for U.S. data transfers with immediate effect, the statement most noteworthy calls into question even Binding Corporate Rules, Standard Contractual Clauses and consent of the data subject as valid means for when applied without any consideration of the actual effectiveness of the protection for the rights of the data subjects.

**On 20 October 2015**: The US House of Representatives agreed to move forward the Judicial Redress Act (JRA) which would ensure some foreigners the right to pursue their privacy rights in US courts. There was strong bipartisan support for the bill which was introduced in March 2015 and will now go to the Senate. The Judicial Redress Act (H.R. 14299) authorizes the Department of Justice (DOJ) to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records maintained by an agency.

**On 16 October 2015**: The EU data protection authorities assembled in the Article 29 Working Party released a statement on the ruling of the Court of Justice of the European Union (CJEU) in the Schrems case (C-362-14) and highlighted the indispensability of a robust, collective and common position on the implementation of the judgment. Hence, the Working Party will continue its analysis on the impact of the CJEU judgment. Until further notice, Standard Contractual Clauses and Binding Corporate Rules can still be used. But transfers that are still taking place under the Safe Harbour decision are considered unlawful. If by the end of January 2016, no appropriate solution is found with the U.S. authorities, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions.

**On 6 October 2015**: The Court of Justice of the European Union (CJEU) released the eagerly awaited judgement in the Schrems case (C-362/14) and found a) that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life b) that safe harbour scheme enables interference, by U.S. public authorities, with the fundamental rights of persons and c) that the existence of a Commission decision finding cannot eliminate or even reduce the powers available to the national supervisory authorities and d) that supervisory authorities have actually the duty to examine relevant complaints with all due diligence but e) that the CJEU it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid.

**On 28 September 2015**: United States Mission to the European Union commented on the opinion of Advocate General Yves Bot in the Schrems case. The respective comment questions the allegations regarding U.S. intelligence practices as well as the finding of Safe Harbor not being adequate. Furthermore, the comment highlights the importance of Safe Harbor for EU and U.S. citizens and
businesses, and the willingness to work closely with the EU Commission to improve the Safe Harbor Framework.

**On 23 September 2015:** With some delay, Advocate General at the Court of Justice of the European Union (CJEU) Yves Bot released his opinion in the Schrems case C-362/14. He found that a) mass surveillance systems used by the United States lead to interference with fundamental rights of EU citizen with regard to their privacy; b) Safe Harbor does not provide adequate protection for EU citizens against this interference and is actually invalid, and c) the EU Commission decision of Safe Harbor Adequacy does have the effect of preventing national authorities from investigating a complaint alleging that a third country does not ensure an adequate level of protection and, where appropriate, from suspending the transfer of that data. Although considered highly influential, the Advocate General’s opinion is not binding on the Court of Justice which has announced give its own judgment in this case on 6 October 2015.

**On 8 September 2015:** EU Commission published a fact sheet with frequently asked questions answers regarding the so-called “Umbrella Agreement” which intends to put in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation. The Agreement covers all personal data exchanged between the EU and the U.S. and required safeguards for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.

**On 24 March 2015:** The European Court of Justice has started to hear the case referred by the Irish High Court on the NSA/PRISM spy scandal which may have major implications for the Safe Harbor Framework and US internet companies operating in Europe (case number: C-362/14). The plaintiff, the Austrian Facebook user Max Schrems, argues that the United States does not provide the “adequate protection” and even claims that the NSA’s PRISM program and other forms of US surveillance are the exact antithesis of “adequate protection”. The expected date for the opinion of the Advocate General is the 24 June 2015.

**On 19 March 2015:** The Data Protection Authorities of Germany passed a resolution which determines that the Safe Harbor decision of the European Commission does not provide sufficient protection for the fundamental rights of data subjects in transfers of personal data to US. They stressed once again their previous statement in 2010 that the data exporter is responsible for “adequate protection” and that self declared certifications pursuant to the Safe Harbor principles are not sufficient.

**On 2 March 2015:** In the “Privacy Perspectives” section of the IAPP website Ernst O. Wilhelm’s well renowned article “Safe Harbor: Caught Between Scylla and Charybdis?” is published which is considered as “first article I have read that succinctly captures the essence of the problems confronting cross-border data flows with respect to data protection and privacy between the U.S. and the EU” by the the former director of the U.S.-EU and Swiss Safe Harbor Frameworks, Damon Greer.

**On 28 January 2015:** At a meeting on the occasion of the 9th European Data Protection Day the Conference of the Data Protection Commissioners of the Federation and the Federal States of Germany were concerned with the phenomenon of the partners on both sides of Atlantic who are becoming increasingly alienated over differences in legal cultures and in matters of data protection. The German DPAs discussed to measures to protect the rights of data subjects in transfers of personal data from the EU to the U.S. based on Safe Harbour including initiating administrative proceedings against relevant companies.
On 27 January 2015: German DPA Voßhoff fully supports the statement of EU Commissioner Andrus that Safe Harbour is not secure and demands short term resolution of EU concerns in transatlantic transfers of personal data. A failure of negotiations may result in the suspension of data transfers to U.S. by the Data Protection Authorities with significant economic effects.

On 22 January 2015: At the Computers, Privacy and Data Protection Conference in Brussels, Paul Nemitz, director for fundamental rights and union citizenship at the European Commission discussed Safe Harbour with U.S. FTC Commissioner Julie Brill.

On 19 November 2014: At the IAPP Data Protection Congress in Brussels, Article 29 Working Party Chairwoman Isabelle Falque-Pierrotin discussed Safe Harbor with U.S. FTC Commissioner Julie Brill. “We want clear answers on what has been brought about by the Snowden revelations,” Falque-Pierrotin said. "DPAs are expecting real answers. We will be very vigilant,” she noted with regard to the 13 recommendations of the European Commission on Safe Harbour. Brill countered, however, that only 11 of the recommendations are under her purview, and the other two are outside of the FTC’s, as well as European Commission’s, remit.

On 17 November 2014: TRUSTe settled FTC charges that it deceived consumers through its privacy seal program which assures consumers that businesses’ practices are in compliance with specific privacy standards like the Safe Harbour Framework. The FTC’s complaint alleges that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in more than 1,000 incidences.

On 9 October 2014: German DPAs published a guide for Cloud Computing highlighting the full liability of the cloud client for all damages done to the data subject by the cloud provider and its agents and advising the cloud client to insist on EU Model Clauses or Binding Corporate Rules in case of doubts that the cloud provider is fully compliant with the Safe Harbour Privacy principles.

On 7 October 2014: Commissioner-designate for the Digital Internal Market, Andrus Ansip, stated in the EU Parliament that, "We must protect everyone’s privacy. Data protection will be an important cornerstone of the Digital Internal Market but Safe Harbour is not secure." He said he would not rule out suspending the so-called Safe Harbour Agreement with the United States, "which has yet to live up to its name."

On 8 August 2014: The Center for Digital Democracy published a complaint on 30 U.S. companies failing to protect European privacy. The complaint, filed at the U.S. Federal Trade Commission (FTC), details how these companies are compiling, using and sharing EU consumers’ personal information without their awareness and meaningful consent, in violation the Safe Harbour framework.

On 10 April 2014: The Article 29 Working Party confirmed all 13 recommendations of the European Commission to improve functioning of the Safe Harbour scheme, in particular recommendations 12: Privacy policies of self-certified companies should include information on the extent to which U.S. law allows public authorities to collect and process data transferred under the Safe Harbour, and 13: National security exceptions used only to an extent that is strictly necessary or proportionate.
**On 12 March 2014:** EU Parliament called for the "immediate suspension" of the Safe Harbour privacy principles stating that these principles “do not provide adequate protection for EU citizens” and urging the U.S. to propose new personal data transfer rules that meet EU data protection requirements.

**On 28 January 2014:** Then EU Commission Vice President Viviane Reding explained at CEPS in Brussels that “We kicked the tires and saw that repairs are needed. For Safe Harbour to be fully roadworthy the U.S. will have to service it. This summer, we will see how well those repairs were carried out. Safe Harbour has to be strengthened or it will be suspended.”

**On 27 November 2013:** The European Commission published a memorandum including 13 recommendations to improve the functioning of the Safe Harbour scheme on the basis of a thorough analysis and consultations with companies. The Commission is calling on U.S. authorities to identify remedies by summer 2014. The Commission will then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations.

**On 24 July 2013:** Following the revelations on U.S. surveillance programs, German DPAs expressed their deep concerns that “there is a substantial likelihood that the principles in the Commission’s decisions are being violated” and pointed out, “Companies that send personal data to the U.S. bear the responsibility for these data. Like everyone in Germany, they must therefore have an interest in ensuring that personal data flows are not subject to large-scale surveillance by intelligence services.”

**On 19 July 2013:** Then EU Commission Vice President Viviane Reding stated at the Justice Council in Vilnius "The Safe Harbour agreement may not be so safe after all. It could be a loophole for data transfers because it allows data transfers from EU to U.S. companies—although U.S. data protection standards are lower than our European ones." Reding announced a solid assessment of the Safe Harbour Agreement which will be presented before the end of the year.

**On 19 March 2012:** EU Commission Vice President Viviane Reding and U.S. Commerce Secretary John Bryson released a Joint Statement on Privacy acknowledging that while regulatory regimes may differ between the U.S. and EU, the common principles at the heart of both systems provide a basis for advancing their dialog to resolve shared privacy challenges and a mutual interest in an enhanced EU-U.S. dialogue.

**On 29 April 2010:** German Data Protection Authorities issued a decision requesting companies transferring data from Europe to the U.S. to actively check that companies in the U.S. importing data actually comply with Safe Harbour Privacy Principles and recommending that “at least the exporting company must determine whether the Safe Harbour certification by the importer is still valid.”

**On 26 July 2000:** The European Commission adopted the “Safe Harbour Adequacy Decision” recognizing the "Safe Harbour Privacy Principles" and "Frequently Asked Questions" issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of relevant personal data transfers from the EU to the U.S.

**On 16 May 2000:** The EU Article 29 Data Protection Working Party adopted an opinion on the level of protection provided by the “Safe Harbor Principles” highlighting in its conclusions that the proposed adequacy finding of U.S. Safe Harbour refers to a system that is not yet operational and that there is a need that any adequacy finding on the Safe Harbour has to be reviewed in the light of experience.