



The EU-US Privacy Shield is a framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. One of its purposes is to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens. The EU-US Privacy Shield is a replacement for the International Safe Harbor Privacy Principles, which were declared invalid by the European Court of Justice in October 2015. In October 2015 the European Court of Justice declared the previous framework called the International Safe Harbor Privacy Principles invalid. Soon after this decision the European Commission and the U.S. Government started talks about a new framework and on 2 February 2016 they reached a political agreement. The European Commission published a draft “adequacy decision”, declaring principles to be equivalent to the protections offered by EU law. The Article 29 Data Protection Working Party delivered an opinion on April 13, 2016, stating that the Privacy Shield offers major improvements compared to the Safe Harbour decisions, but that three major points of concern still remain. They relate to deletion of data, collection of massive amounts of data, and clarification of the new Ombudsperson mechanism. The European Data Protection Supervisor issued an opinion on 30 May 2016 in which he stated that "the Privacy Shield, as it stands, is not robust enough to withstand future legal scrutiny before the Court". On 8 July 2016 EU Member States representatives (article 31 committee) approved the final version of the EU-U.S. Privacy Shield, paving the way for the adoption of the decision by the Commission. The European Commission adopted the framework on 12 July 2016 and it went into effect the same day. U.S. President Donald Trump signed an Executive Order entitled "Enhancing Public Safety" which states that U.S. privacy protections will not be extended beyond US citizens or residents: Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information. The European Commission has stated that: The US Privacy Act has never offered data protection rights to Europeans. The Commission negotiated two additional instruments to ensure that EU citizens’ data is duly protected when transferred to the US: The EU-US Privacy Shield, which does not rely on the protections under the US Privacy Act. The EU-US Umbrella Agreement, which enters into force on 1 February (2017). To finalise this agreement, the US Congress adopted a new law last year, the US Judicial Redress Act, which extends the benefits of the US Privacy Act to Europeans and gives them access to US courts.” The Commission said it will “continue to monitor the implementation of both instruments”. German MEP Jan Philipp Albrecht and campaigner Max Schrems have criticized the new ruling, with the latter predicting that the Commission might be taking a "round-trip to Luxembourg" (where the European Court of Justice is located). EU Commissioner for Consumers, Vera Jourova, expressed confidence that a deal would be reached by the end of February. Many Europeans are demanding a mechanism for individual European citizens to lodge complaints over the use of their data, as well as a transparency scheme to assure that European citizens data does not fall into the hands of U.S intelligence agencies.....

GDPR US-EU Privacy Regulations

Europe’s new data privacy and security law describes your obligation regarding rectification or erasure of personal data or restriction of processing. We are entitled to request you to erase any personal data you hold about me under EU (GDPR). Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it’s relatively easy to ID someone from it. <https://gdpr.eu/what-is-gdpr/>