International Safe Harbor Privacy Principles

This article is about the first framework, invalidated in 2015. For the superseding framework, also found invalid, see EU–US Privacy Shield. For the current framework, see EU–US Data Privacy Framework.

The International Safe Harbor Privacy Principles or Safe Harbour Privacy Principles were principles developed between 1998 and 2000 in order to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information. They were overturned on October 6, 2015, by the European Court of Justice (ECJ), which enabled some US companies to comply with privacy laws protecting European Union and Swiss citizens. US companies storing customer data could self-certify that they adhered to 7 principles, to comply with the EU Data Protection Directive and with Swiss requirements. The US Department of Commerce developed privacy frameworks in conjunction with both the European Union and the Federal Data Protection and Information Commissioner of Switzerland.

Within the context of a series of decisions on the adequacy of the protection of personal data transferred to other countries, the European Commission made a decision in 2000 that the United States' principles did comply with the EU Directive – the so-called "Safe Harbour decision". However, after a customer complained that his Facebook data were insufficiently protected, the ECJ declared in October 2015 that the Safe Harbour decision was invalid, leading to further talks being held by the Commission with the US authorities towards "a renewed and sound framework for transatlantic data flows".

The European Commission and the United States agreed to establish a new framework for transatlantic data flows on 2 February 2016, known as the "EU–US Privacy Shield", which was closely followed by the Swiss-US Privacy Shield Framework.

Background history

In 1980, the OECD issued recommendations for protection of personal data in the form of eight principles. These were non-binding and in 1995, the European

Union (EU) enacted a more binding form of governance, i.e. legislation, to protect personal data privacy in the form of the Data Protection Directive.

According to the Data Protection Directive, companies operating in the European Union are not permitted to send personal data to "third countries" outside the European Economic Area, unless they guarantee adequate levels of protection, "the data subject himself agrees to the transfer" or "if Binding corporate rules or Standard Contractual Clauses have been authorised." The latter means that privacy protection can be at an organizational level, where a multinational organization produces and documents its internal controls on personal data or they can be at the level of a country if its laws are considered to offer protection equal to the EU.

The Safe Harbour Privacy Principles were developed between 1998 and 2000. Key player was the Art. 29 Working Party, at that time chaired by the Italian Data Protection Authority www.garanteprivacy.it President Prof. Stefano Rodotà, one of the fathers of the privacy framework in Europe, helped by the Italian Data Protection Authority Secretary General Mr. Giovanni Buttarelli, lately appointed as European Data Protection Supervisor (EDPS). Safe Harbour Principles were designed to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information. US companies could opt into a program and be certified if they adhered to seven principles and 15 frequently asked questions and answers per the Directive. In July 2000, the European Commission (EC) decided that US companies complying with the principles and registering their certification that they met the EU requirements, the so-called "safe harbour scheme", were allowed to transfer data from the EU to the US. This is referred to as the Safe Harbour decision.

On 6 October 2015, the European Court of Justice invalidated the EC's Safe Harbour Decision, because "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" (boldened in original text).

According to the European Commission, the EU–US Privacy Shield agreed on 2 February 2016 "reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid. The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission, including through increased cooperation with European Data Protection Authorities. The new arrangement includes commitments by the U.S. that possibilities under U.S. law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalised access. Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson".

Principles

The seven principles from 2000 are:

Notice – Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.

Choice – Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.

Onward Transfer – Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

Security – Reasonable efforts must be made to prevent loss of collected information.

Data Integrity – Data must be relevant and reliable for the purpose it was collected.

Access – Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.

Enforcement – There must be effective means of enforcing these rules.

Scope, certification and enforcement

Only U.S. organizations regulated by the Federal Trade Commission or the Department of Transportation may participate in this voluntary program. This excludes many financial institutions (such as banks, investment houses, credit unions, and savings & loans institutions), telecommunication common carriers (including internet service providers), labor associations, non-profit organizations, agricultural co-operatives, and meat processors, journalists and most insurances, although it may include investment banks.

After opting in, an organization must have appropriate employee training and an effective dispute mechanism in place, and self re-certify every 12 months in writing that it agrees to adhere to the U.S.–EU Safe Harbor Framework's principles, including notice, choice, access, and enforcement. It can either perform a self-assessment to verify that it complies with the principles, or hire a third-party to perform the assessment. Companies pay an annual $100 fee for registration except for first time registration ($200).

The U.S. government does not regulate Safe Harbor, which is self-regulated through its private sector members and the dispute resolution entities they pick. The Federal Trade Commission "manages" the system under the oversight of the U.S. Department of Commerce. To comply with the commitments, violators can be penalized under the Federal Trade Commission Act by administrative orders and civil penalties of up to $16,000 per day for violations. If an organization fails to comply with the framework it must promptly notify the Department of Commerce, or else it can be prosecuted under the 'False Statements Act'.

In a 2011 case, the Federal Trade Commission obtained a consent decree from a California-based online retailer that had sold exclusively to customers in the United Kingdom. Among its many alleged deceptive practices was representing itself as having self-certified under Safe Harbour when in fact it had not. It was barred from using such deceptive practices in the future.

Criticism and evaluation

EU evaluations

The EU–US Safe Harbour Principles 'self certification scheme' has been criticised in regard to its compliance and enforcement in three external EU evaluations:

A 2002 review by the European Union found "a substantial number of organisations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies" and that "not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbour rules and not all have in place privacy practices applicable to themselves."

2004 review by the European Union:

In 2008, an Australian consulting company named Galexia issued a scathing review, finding "the ability of the US to protect privacy through self-regulation, backed by claimed regulator oversight was questionable'. They documented basic claims as incorrect where only 1109 out of 1597 recorded organisations listed by the US Department of Commerce (DOC) on 17 October 2008 remained in the database after doubles, triples and 'not current' organisations were removed. Only 348 organisations met even the most basic requirements for compliance. Of these, only 54 extended their Safe Harbor membership to all data categories (manual, offline, online, human resources). 206 organisations falsely claimed to be members for years, yet there was no indication that they were subject of any US enforcement. Reviewers criticized the DOC's 'Safe Harbor Certification Mark' offered to companies to use as a "visual manifestation of the organization when it self-certifies that it will comply" as misleading, because it does not carry the words "self certify" on it. Only 900 organizations provided a link to their privacy policies, for 421 it was unavailable. Numerous policies were only 1-3 sentences long, containing "virtually no information". Many entries appeared to confuse privacy compliance with security compliance and showed a "lack of understanding about the Safe Harbor program". The companies' listing of their dispute resolution providers was confusing, and problems regarding independence and affordability were noted. Many organisations did not spell out that they would cooperate with or explain to their customers that they could choose the dispute resolution panel established by the EU Data Protection Authorities.

Galexia recommended the EU to re-negotiate the Safe Harbor arrangement, provide warnings to EU consumers and consider to comprehensively review all list entries. They recommended to the US to investigate the hundreds of organisations making false claims, revising its statements about the number of participants, to abandon the use of the Safe Harbor Certification Mark, to investigate the unauthorised and misleading use of its Departmental logo and

automatically suspend an organisation’s membership if they failed to renew their Safe Harbor certification.

Patriot Act's reach

In June 2011, Microsoft U.K.'s managing director Gordon Frazer said that "cloud data, regardless of where it is in the world, is not protected against the Patriot Act."

The Netherlands promptly ruled out U.S. cloud suppliers from Dutch government contracts, and even considered a ban on Microsoft- and Google-provided cloud contracts. A Dutch subsidiary of the U.S. based Computer Sciences Corporation (CSC) runs the electronic health records of the Dutch national health service system and warned, that unless CSC could assure it was not subject to the Patriot Act, it would end the contract.

One year later in 2012, a legal research paper supported the notion that the Patriot Act allowed U.S. law enforcement to bypass European privacy laws.

Citizen complaint about Facebook data safety

In October 2015, the ECJ responded to a referral from the High Court of Ireland in relation to a complaint from Austrian citizen Maximillian Schrems regarding Facebook's processing of his personal data from its Irish subsidiary to servers in the US. Schrems complained that "in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities". The ECJ held the Safe Harbour Principles to be invalid, as they did not require all organizations entitled to work with EU privacy-related data to comply with it, thus providing insufficient guarantees. US federal government agencies could use personal data under US law, but were not required to opt in. The court held that companies opting in were "bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with national security, public interest and law enforcement requirements".

In accordance with the EU rules for referral to the ECJ for a 'preliminary ruling', the Irish Data Protection Commissioner since then has had to "examine Mr. Schrems's case 'with all due diligence' and ... decide whether ... the transfer of Facebook's European subscribers' personal data to the United States should be suspended".[1] EU regulators said that if the ECJ and United States did not negotiate a new system within three months, businesses might face action from European privacy regulators. On October 29, 2015, a new "Safe Harbour 2.0" agreement appeared close to being finalized.[24] However Commissioner Jourova expected the U.S. to act next.[25] American NGOs were quick to expand on the significance of the decision.

This section needs to be updated. Please help update this article to reflect recent events or newly available information. (April 2020)

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 were 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 did not fall into the hands of U.S intelligence agencies. The Article 29 Working Party has taken up this demand, and stated it would hold back another month until March 2016 to decide on consequences of Commissioner Jourova's new proposal. The European Commission’s Director for Fundamental Rights Paul Nemitz stated at a conference in Brussels in January how the Commission would decide on the "adequacy" of data protection. The Economist newspaper predicts that "once the Commission has issued a beefed-up 'adequacy decision', it will be harder for the ECJ to strike it down." Privacy activist Joe McNamee summed up the situation by noting the Commission has announced agreements prematurely, thus forfeiting its negotiating right. At the same time, the first court challenges in Germany have commenced: the Hamburg data protection authority was during February 2016 preparing to fine three companies for relying on Safe Harbour as the legal basis for their transatlantic data transfers and two other companies were under investigation. From the other side a reaction looked imminent.

On 25 March 2021 the European Commission and US Secretary of Commerce reported that "intensified negotiations" were taking place. Discussions continued at the U.S.-EU Summit in Brussels in June 2021.