PRIVACY SHIELD – OVERVIEW

ABSTRACT

The aim of this paper is to give an overview on the Privacy Shield Framework. This agreement, which is effective from 12 July 2016, follows the requirements stated in the decision of the European Court of Justice, known as "Schrem" case[1], where the Court invalidated the Safe Harbour agreement. The new program strictly regulates personal data flows between the E.U. and the U.S.; moreover, it represents a tool, along with Standard Contractual Clauses and Binding Corporate Rules, that allows companies to legally transfer personal data between the two side of the Atlantic. The program in question acknowledges the fundamental value of personal information in the modern digital economy and its purpose is to strenghten the relationship between the E.U. and the U.S. The brief analysis below aims to highlight the fact that doing the self-certification can be an important step for a company in order to comply with the legal requirements related to the protection of E.U. personal data transferred in the U.S. because the European Commission adopted an "adequacy" decision in which the Privacy Shield agreement is declared to be an appropriate tool for this scope.

What is the Privacy Shield agreement?

The E.U.-U.S. Privacy Shield Framework, which is effective from 12 July 2016, is an agreement that was designed by the U.S. Department of Commerce and the European Commission to provide EU, U.S. companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States with the aim to support transatlantic commerce.

Which kind of businesses can self-certify to the program?

It is crucial to state the fact that the Framework applies when European data controllers or data processor transfer personal data to U.S. companies self-certified to the Privacy Shield; therefore it should be clear that only this specific kind of data-flow is concerned by the agreement.
Moreover, it should be pointed out that not every U.S. company could join the program; only U.S. organizations that are currently subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are able to self-certify. This means that organizations such as banks, federal credit unions, and savings & loan institutions, telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organizations, most packer and stockyard activities and some insurance activities are excluded to the program.

Which type of data are concerned by this Framework?

In the Framework's text (available at https://www.privacyshield.gov/EU-US-Framework) personal data or personal information are defined as "data about an identified or identifiable individual that are within the scope of the Directive 95/46/CE, received by an organization in the United States from the European Union, and recorded in any form." Specifically, personal data can be "any information concerning natural persons that are or

[1] Decision of the European Court of Justice in case C 362/14 Maximillian Schrems v Data Protection Commissioner. The judgement was issued on 5th October 2016.

WWW.PEZZILAW.COM - MAIL@PEZZILAW.COM

TEL +39.051.580382/581338 FAX: +39.051.334850

PARTITA I.V.A.- C.F.: 02322171204

can be identified also by way of other items of information – e.g., via a number or an ID code. For instance, personal data is one's first or last name, address, Tax ID as well as a picture, the recording of one's voice or one's fingerprint, or medical, accounting or financial information relating to that person."[2]

Why a company should join the Privacy Shield?

Even if the adherence to the Privacy Shield certification happens on a voluntary base, nonetheless companies that usually process personal data of E.U. subjects should into serious consideration the fact they are required to meet all E.U. data protection laws; therefore doing the self-certification to the framework in question would be an important step in order to comply with these kind of laws. Moreover, since the agreements in question were deemed as 'adequate' by the European Commission (and by the Swiss Government), all the member States of the EU (and Switzerland) are bound to them. This fact should be highly considered by companies that have to choose between self-certifiying with the Privacy Shield procedure and mainting (or adopting) different tools such as Standard Contractual Clauses[3] or Binding Corporate Rules[4].
In addition to this, another important benefit lies in the fact that there will be no need for an organization to fulfill the requirements for prior approval of data transfers prescribed by EU member States because the approval will be automatically awarded. Finally, since the compliance requirements are cost-effective, this would probably mean that also small and medium-sized businesses will benefit from this fact.

How are the transfers of data within a controlled group of corporations or between controllers treated by the Privacy Shield?

Specific requirements are defined in the Framework for these situations. As for the former, lett. b), art. 10, 3rd par. states that "a contract is not always required (…). Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (e.g., compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the Privacy Shield organization remains responsible for compliance with the Principles." As for the latter, lett. c) of the same provision says that "(...) the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. The Privacy Shield organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield, not including the requirement that the third party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism."

How to join the program?

2 Cit. http://www.garanteprivacy.it/web/guest/home_en/data-protection-and-privacy-glossary

3 Standard Contractual Clauses are sets of standard clauses issued by the European Commission on the basis of articles 26, par. 4 and 26, par. 2 of the Directive 95/46/EC; they provide model clauses for transfers from data controllers to data controllers and for the tranfers form data controllers to processor located outside the E.U.; the two sets of Standard Contractual Clauses can be found at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm .

4 Binding Corporate Rules are tools adopted by multinational group of companies (such as Code of Practice/Conduct) with the aim to establish a global policy related to transfer of personal information within the same corporation to entities situated in countries where an adequate level of protection of this kind of data is not provided.

WWW.PEZZILAW.COM - MAIL@PEZZILAW.COM

TEL +39.051.580382/581338 FAX: +39.051.334850

PARTITA I.V.A.- C.F.: 02322171204

In order to join the Privacy Shield Program, which is administered by the International Trade Administration within the U.S. Department of Commerce, a U.S.-based organization will be required to self-certify annually to the Department of Commerce its adherence to the Privacy Shield principles via website (https://www.privacyshield.gov) and publicly commit to comply with the Framework's requirements. It must be highlighted not only the fact that joining the Privacy Shield Framework is voluntary, but also the circumstance that, once an eligible organization shows public commitment with the Framework's principles, its commitment will become enforceable under U.S. Law.

IN A NUTSHELL, TO JOIN THE PRIVACY SHIELD PROGRAM AN ORGANIZATION SHOULD: 1) PRODUCE A CONFORMING PRIVACY POLICY; 2) CLEARLY IDENTIFY AN INDEPENDENT RECOURSE MECHANISM; 3) MAKE THE SELF-CERTIFICATION TROUGH THE PRIVACY SHIELD OFFICIAL WEBSITE (SEE THE LINK PROVIDED ABOVE)

Below a description of the fundamental steps that a company needs to undertake in order to join the program:

- First of all, check the organization's eligibility to participate in the Privacy Shield;
- After that, your organization should develop a privacy policy **before** the presentation of the self-certification to the Department of Commerce[5]. This is the most relevant step that requires a particular focus and reference with the Privacy Shield Principles. Note that this document should include a description of the organization's own business operations. Moreover, the policy should clearly state that the organization adheres to the Privacy Shield Principles and the policy itself should be comprehensible and concise;
- then there is the need to define the organization's indipendent rechourse mechanism. This mechanism that a self-certify companies need to provide prior to self-certification should be able to examine unresolved complaints without any additional cost for individuals.[6] Different programs could be used: private-sector dispute resolutions solutions could be an option; moreover, organizations may decide to cooperate with E.U. data protection authorities;[7]
- pay the required fee to the International Centre for Dispute Resolution-American Arbitration Association responsible for Binding Arbitration Mechanism;
- make sure that organization's verification mechanism is in place: this requirement allows organizations that undertake the self-certification procedure to choose to verify their compliance either through self-assessment or outside compliance reviews;
- Identification of a contact within the organization regarding Privacy Shield: it is important to consider the fact that companies are required to answer to individuals' complaints within 45 days of receiving such claims.

[5] It is also fundamental to mention that, prior to the self-certification, the effectiveness of the privacy policy should be checked.

[6] See the entire art. 11, 3rd par. of the Framework for all the detailed requirements of the mechanism in question.

[7] In addition to this, companies should bear in mind that, if human resources data are concerned, they must agree to cooperate with E.U. data protection authorities. When making practical use of these kind of authorities an annual fee has to be paid too.

- Fill in all the information required by the self-certification form before submitting the self-certification to the Department of Commerce.

Which are the main principles of the Framework?

Organizations with the aim to apply for the Privacy Shield needs to adhere and comply with all the principles stated in the Framework; the most relevant are: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement and liability.

It is worth mentioning here the article related to the notice principle because it provides a list of the main duties of a company self-certified to the Privacy Shield; indeed, according to par. 2, art. 1 of the Privacy Shield, an organization must inform individuals about:

i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,
iv. the purposes for which it collects and uses personal information about them,
v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
vi.the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
vii. the right of individuals to access their personal data,
viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,
xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,
xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
xiii. its liability in cases of onward transfers to third parties.

b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

What about companies relying on the Safe Harbour Agreement?

The process that brought to the adoption of the Privacy Shield started with the decision given by the European Court of Justice in the Schrems case; indeed, this Court in the judgement just cited deemed as invalid the

WWW.PEZZILAW.COM - MAIL@PEZZILAW.COM

TEL +39.051.580382/581338 FAX: +39.051.334850

PARTITA I.V.A.- C.F.: 02322171204

European Commission's decision on the E.U.-U.S. agreement regarding data transfer regime known as "Safe Harbour". Therefore companies that relied on Safe Harbour and now willing to self-certify to the Privacy Shield must remove any reference to the former (prior to attend the self-certification procedure).

There are also some pros and cons for companies that relied on the Safe Harbour certification. Indeed, for these organizations the transition to the Privacy Shield would be easier because of the relationship between the requirements of the two frameworks, even if the new conditions are more strict. On the other hand, a consideration needs to be affirmed concerning the fact that an organization self-certified to the Safe Harbour undertook some important costs in order to comply with that mechanism and then adopt different tools after its invalidation by the European Court of Justice. Now, if the company that suffered this situation aims to adopt the Privacy Shield certification, it will need to take into account the circumstance that a revision of the agreements with service providers, third-parties and its privacy policy will be required in to meet the conditions affirmed by the new principles.

(updated Oct. 30, 2017)

Claudio Pezzi - Lorenzo Zandonatti
PEZZI & ASSOCIATI LAW FIRM
Bologna - Milano
www.pezzilaw.com