16/EN
WP 245

EU-US PRIVACY SHIELD
F.A.Q. FOR EUROPEAN BUSINESSES

Adopted on 13 December 2016

EU-US PRIVACY SHIELD
F.A.Q. FOR EUROPEAN BUSINESSES

Q1. What is the EU-U.S. Privacy Shield?

The EU-U.S. Privacy Shield[1] is a self-certification mechanism for U.S. based companies that has been recognized by the European Commission as providing an adequate level of protection for personal data transferred from an EU entity to U.S. based self-certified companies and thus as an element for offering legal guarantees for such data transfers.
Here are some relevant links for more information:

- The Adequacy decision as published in the official Journal of the EU
- The Guide to the EU-US Privacy Shield developed by the European Commission
- The Privacy Shield program website as administrated by the US Department of Commerce.

Q2. Which US companies are eligible to the EU-U.S. Privacy Shield?

In order to be entitled to self-certify to the Privacy Shield, an U.S. based company must be subject to the investigatory and enforcement powers of the Federal Trade Commission ("FTC") or of the Department of Transportation ("DoT"). Other U.S. statutory bodies may be included in the future.

This means that, for example, non-profit organizations, banks, business of insurances and telecommunication service providers (with regard to common carrier activities) do not fall under the jurisdiction of the FTC or DoT and therefore cannot self-certify under the Privacy Shield.

The Privacy Shield applies to any type of personal data transferred from an EU entity to the US including commercial, health or human resource related data, as long as the recipient US Company has self-certified to the Framework.
You might find additional information on https://www.privacyshield.gov/

[1] The decision on the adequacy of the EU-U.S. Privacy Shield Framework ("Privacy Shield") or ("Framework") was adopted by the European Commission on July 12, 2016. It was designed by the European Commission and the U.S. Department of Commerce to replace the Safe-Harbor-Decision 2000/520/EC which were declared invalid by the European Court of Justice in 6 October 2015.

Q3. What to do before transferring personal data to a U.S. based company which is or claims to be Privacy Shield certified?

Before transferring personal data to a U.S. based company which claims to be Privacy Shield certified, European businesses also have to ascertain that the U.S. based company holds an active certification (certifications need to be renewed annually) and that the certification covers the data in question (in particular: HR data, respectively, Non-HR data).

To verify whether or not a certification is active and applicable, European companies need to consult the Privacy Shield List, published on the U.S. Department of Commerce's website (https://www.privacyshield.gov/welcome).

All U.S. based companies having successfully completed the self-certification process are listed. The Privacy Shield List also provides information on the types of personal data a U.S. based company has certified for (HR or non-HR data) and provides details on the services it offers.

The US Department of Commerce is also listing companies that are no longer members of the Privacy Shield. Those companies are not allowed to receive personal data of EU individuals under the Privacy Shield after the end of their participation, but have to continue to apply the Privacy Shield principles to data transferred while their participation was active.
For the transfer of personal data to companies that are not or no longer members of the Privacy Shield, other EU approved transfer mechanisms such as Binding Corporate Rules, Standard Contractual Clauses, may be used for the transfer of personal data of EU individuals to U.S. based businesses.

The fact that the recipient in US is member of the EU-US privacy Shield will enable European businesses to comply with the national laws implementing article 25 of the EC Directive 95/46, but all other requirements as set up by the national data protection law remain applicable;

- For transfers to U.S. based company acting as controller

Before transferring personal data, European businesses acting as Controllers need to ensure compliance of the transfer with applicable data protection law. In the first step, European businesses can only share personal data with a U.S. based company if the transfer will benefit from a legal basis (i.e. if it complies with national law implementing articles 7 and 8 of the EC Directive 95/46/EC). Moreover, all other general requirements from EU data protection law towards the data transfer/s need to be met (e.g. purpose limitation, proportionality, quality, information obligations towards data subjects). If data is to be transferred to a certified U.S. based company, the European business transferring the data also needs to inform the data subjects about the identity of the recipients of their data and about the fact that the data benefits from protection by the Privacy Shield.
European businesses should take note that commercial contractual clauses (e.g. with their business partners) could restrict them in their possibilities to transfer personal data to other businesses outside the EU or EEA.

- For transfers to U.S. based company acting as processor

When a European based company acting as data controller transfers data to a U.S. based data processor, acting on its behalf for processing purposes only (storage, IT maintenance, helpdesk etc.), according to Art. 17 of EC Directive 95/46/EC the two companies are obliged to conclude a data processing contract regardless of whether the data processor is a member of the Privacy Shield or not.

The conclusion of a contract is required in order to ensure that the U.S. data processor commits to:

- act only on instructions received from the data controller;

- provide appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed[2]. Having regard to the state of the art and the cost of their implementation, such security measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. ; and

- by taking into account the nature of the processing, assists the controller in responding to individuals exercising their right to access their personal data.

Please note that under the EU Data Protection Directive national, data protection law may impose additional requirements, for example require EU businesses to include additional content into their data processing contracts. Your national Data Protection Authority can provide you with further guidance.

For instance, it is advisable that the EU Business indicates if it agrees or not that the US processor may sub process the personal information to third party processors and the applicable conditions (in terms of transparency, liability). Moreover, it might also be useful for the EU Business to get assurance about the notification of security breaches and commitments about deletion of the data once the service contract is terminated.

Q4. Where can I find guidance regarding the registration of US subsidiary companies of European businesses?

For information on the registration of US subsidiary companies of European businesses in the Privacy Shield, please visit the U.S. Department of Commerce corresponding webpage: (https://www.privacyshield.gov/article?id=U-S-Subsidiaries-of-European-Businesses-Participation-in-Privacy-Shield).

Registration to the Privacy Shield is available on the U.S. Department of Commerce website (https://www.privacyshield.gov/welcome).

[2] For more information on onward transfers by U.S. based data processors, please visit the section "*Obligatory Contracts for Onward Transfers*" of the Privacy Shield and see Question 4.

A guide to the self-certification process, is also provided thereby: (https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1).

In any case, data protection principles applying under the Privacy Shield Framework will have to be complied with by the US self-certified entity.