EU-U.S. DATA PRIVACY FRAMEWORK

F.A.Q. FOR EUROPEAN BUSINESSES[1]

Adopted on 16 July 2024

[1] In this context, European businesses refer to businesses in the EEA, which transfer or may transfer personal data to companies in the U.S. certified under the DPF.

Table of contents

Q1. What is the EU-U.S. Data Privacy Framework? 3

Q2. Which U.S. companies are eligible to the EU-U.S. Data Privacy Framework? 3

Q3. What to do before transferring personal data to a company in the U.S. which is, or claims to be certified under the EU-U.S. Data Privacy Framework? 4

Q4. Where can I find guidance regarding the certification of U.S. subsidiary companies of European businesses? 6

Q1. WHAT IS THE EU-U.S. DATA PRIVACY FRAMEWORK?

The EU-U.S. Data Privacy Framework ("DPF") is a self-certification mechanism for companies in the U.S. Companies that have self-certified under the DPF must comply with its principles, rules and obligations related to the processing of personal data of EEA individuals. For more information about these commitments, see the Data Privacy Framework Principles.[2]

The European Commission considered that transfers of personal data from the EEA to companies certified under the DPF enjoy an adequate level of protection.[3] As a result, personal data can be transferred freely to U.S. certified companies, without the need to put in place further safeguards or obtain an authorisation. Here are some relevant links for more information:

- The European Commission's Questions and Answers: Data Privacy Framework[4]
- The Data Privacy Framework website as administrated by the U.S. Department of Commerce[5]
- The European Commission's decision on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework[6]

The DPF applies to any type of personal data transferred from the EEA to the U.S., including personal data processed for commercial or health purposes, and human resources data collected in the context of an employment relationship (hereafter: "HR Data"), as long as the recipient company in the U.S. is self-certified under the DPF to process those types of data.[7]

Q2. WHICH U.S. COMPANIES ARE ELIGIBLE TO THE EU-U.S. DATA PRIVACY FRAMEWORK?

In order to be eligible to self-certify to the DPF, a company in the U.S. must be subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission ("FTC") or of the U.S. Department of Transportation ("DoT"). Other U.S. statutory bodies may be included in the future.[8]

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

[2] https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles

[3] The decision on the adequacy of the Data Privacy Framework was adopted by the European Commission on July 10, 2023. It was designed by the European Commission and the U.S. Department of Commerce to replace the Privacy Shield Decision (EU) 2016/1250 which was declared invalid by the European Court of Justice in 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)*.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[5] https://www.dataprivacyframework.gov/s/

[6] https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

[7] Note that not all DPF self-certifications cover HR Data. It is therefore important to check whether this is the case, if relevant. See also Q3.

[8] See Annex I to the adequacy decision, EU-U.S. Data Privacy Framework Principles issued by the U.S. Department of Commerce, para I.2.

Q3. WHAT TO DO BEFORE TRANSFERRING PERSONAL DATA TO A COMPANY IN THE U.S. WHICH IS, OR CLAIMS TO BE CERTIFIED UNDER THE EU-U.S. DATA PRIVACY FRAMEWORK?

Before transferring personal data to a company in the U.S. which claims to be self-certified under the DPF, a data exporter in the EEA must ascertain that the company in the U.S. holds an active self-certification (certifications must be renewed annually) and that this certification covers the data in question (in particular if it covers HR Data, respectively, non-HR Data).[9]

To verify whether or not a self-certification is active and applicable, data exporters in the EEA need to check if the company in the U.S. is on the Data Privacy Framework List,[10] published on the U.S. Department of Commerce's website. This list also includes a register of companies that have been removed from the List ("inactive participants"), stating the reasons for their removal. An EEA data exporter cannot rely on the DPF for transfers of personal data to such companies. Please note that companies that have been removed from the Data Privacy Framework List must continue to apply the Data Privacy Framework Principles to personal data received while participating in the DPF for as long as they retain these data.

For the transfer of personal data to companies in the U.S. that are not (or no longer) self-certified under the DPF, other grounds for transfer in Chapter V of the GDPR may be used, such as Binding Corporate Rules or Standard Contractual Clauses.

The fact that the recipient in the U.S. is self-certified under the DPF will enable data exporters in the EEA to comply with Chapter V of the GDPR, but all other requirements in the GDPR and any other national data protection law remain applicable.

3.1. Transfers to U.S. subsidiaries of companies certified under the EU-U.S. Data Privacy Framework

In the case of transfers to companies in the U.S. that are subsidiaries of a DPF-certified parent company, EEA data exporters must check if the certification of the parent company also covers the subsidiary company concerned.

You can find additional information on how to verify the scope of an organisation's self-certification, including whether other U.S. entities or U.S. subsidiaries are covered by it, here.[11]

3.2. Transfers to a company in the U.S. acting as a controller

Before transferring personal data to a controller in the U.S., an EEA data exporter must ensure the transfer complies with all relevant provisions of the GDPR. As a first step, the data exporter can only share personal data with a company in the U.S. if there is a legal basis for the processing (Article 6 of the GDPR). Moreover, all other requirements in the GDPR need to be met (e.g. purpose limitation, proportionality, accuracy and information obligations towards data subjects). Note that when data is to be transferred to a self-certified company in the U.S., the EEA data exporter, in accordance with Articles 13 and 14 GDPR, must inform data subjects about the identity of the recipients of their data

[9] See definition of HR Data in Q1.
[10] https://www.dataprivacyframework.gov/list
[11] https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments

and about the fact that the transfer is covered by the EU-U.S. Data Privacy Framework adequacy decision.

3.3. Transfers to a company in the U.S. acting as a processor

When an EEA controller transfers data to a processor in the U.S., the controller and processor are obliged to conclude a data processing agreement under Article 28 GDPR (hereafter: Data processing agreement), regardless of whether the processor is self-certified under the DPF.

You can find more information about the contract requirements for transfers to a processor in the U.S. here.[12]

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

- process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in line with what is required by the data processing agreement (stemming from Article 32 of the GDPR) and sections 4 and 10 of the DPF;
- respect the conditions referred to in the data processing agreement (stemming from paragraphs 2 and 4 of Article 28 of the GDPR) and Section II.3.B of the DPF for engaging another processor;
- taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- assist the controller in ensuring compliance with its obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the processor;
- at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data;
- make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated

[12] https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor

by the controller. With regard to this last point, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the DPF.

Where the U.S. processor engages another processor ("sub-processor") to carry out specific processing activities on behalf of the EEA controller, the processor must ensure that the requirements under Section II.3.B DPF are fulfilled. This includes ensuring that the sub-processor provides the same level of protection of personal data as required in the DPF and the same data protection obligations as set out in the data processing agreement. Where a sub-processor fails to fulfil its data protection obligations, the initial U.S. processor shall remain fully liable to the controller for the performance of that sub-processor's obligations.

Q4. WHERE CAN I FIND GUIDANCE REGARDING THE CERTIFICATION OF U.S. SUBSIDIARY COMPANIES OF EUROPEAN BUSINESSES?

U.S. subsidiaries of EEA businesses can self-certify to the DPF if they are subject to the jurisdiction of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT).

You can find more information on the eligibility requirements here,[13] and a guide to the self-certification process here.[14]

[13] https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program

[14] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931)