

EU-U.S. DATA PRIVACY FRAMEWORK

F.A.Q. FOR EUROPEAN INDIVIDUALS¹

Adopted on 16 July 2024

¹ In this context, European individuals means any natural person, regardless of their nationality, whose personal data have been transferred to a U.S. company under the EU-U.S. Data Privacy Framework.

Table of contents

Q1. What is the EU-U.S. Data Privacy Framework?	3
Q2. How do I benefit from the EU-US Data Privacy Framework?	3
Q3. How do I lodge a complaint?	4
Q4. How will the national DPA handle my complaint?	4

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. The European Commission considered that transfers of personal data from the EEA to companies in the U.S. certified under the DPF enjoy an adequate level of protection.² 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.

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.³

Q2. HOW DO I BENEFIT FROM THE EU-US DATA PRIVACY FRAMEWORK?

The DPF relies on commitments taken by companies in the U.S. to respect its principles, rules and obligations related to the processing of personal data of European individuals. For more information about these commitments, see the [Data Privacy Framework Principles](#).⁴

The DPF grants you certain rights when your personal data have been transferred from the EEA to a company in the U.S. that has self-certified under the DPF. Notably, you have the right to be informed of such a transfer and its purpose, as well as to obtain access to your personal data, and correct or delete any incorrect or unlawfully handled data.⁵ You can verify whether a company in the U.S. has a valid certification by checking the online EU-U.S. [Data Privacy Framework List](#)⁶ on the U.S. Department of Commerce’s website.

If you have any questions or concerns about the processing of your personal data by a company certified under the DPF, you are encouraged to directly contact that company, as a first step.

If your concern is not resolved by the company, or you have reasons to not address it directly to the company, you can contact any EEA national data protection authority (national DPA) and, in particular,

² The decision on the adequacy of the EU-U.S. 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 Maximilian Schrems (Schrems II).

³ Note that not all DPF self-certifications cover HR Data. You may check the scope of a specific company’s certification on the EU-U.S. [Data Privacy Framework List](#) on the U.S. Department of Commerce’s website (<https://www.dataprivacyframework.gov/list>).

⁴[https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-\(DPF\)-Principles](https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles)

⁵ For more detailed information as to the guarantees for the data transferred and as to your rights under the EU-U.S. Data Privacy Framework, please consult the European Commission’s [FAQ on the EU-U.S. Data Privacy Framework](#) (https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) (see, in particular, the answer to Q3).

⁶ <https://www.dataprivacyframework.gov/list>

the one in the country where you reside or work, or from where your personal data has been transferred to the U.S.⁷

Q3. HOW DO I LODGE A COMPLAINT?

If you believe that a company in the U.S. has violated its obligations or your rights under the EU-U.S. Data Privacy Framework, several redress avenues are available to you. Read more about the ways to submit a complaint [here](#).⁸

On the [Data Privacy Framework List](#)⁹ you can find information about the complaint procedure and independent recourse mechanism for each self-certified company.¹⁰

You can always lodge a complaint relating to a U.S. company's compliance with the Data Privacy Framework Principles directly with a national DPA. Please provide the national DPA with as many details on the matter as possible, enabling your DPA to handle your complaint in the best way. A [template complaint form](#)¹¹ (to be used on a voluntary basis) is available for such cases.

You may also contact your national DPA for more information about the ways to submit a complaint.¹²

Q4. HOW WILL THE NATIONAL DPA HANDLE MY COMPLAINT?

When you lodge a complaint with a national DPA, different scenarios may occur:

1- Informal panel of EU DPAs

If your complaint concerns the processing of HR Data¹³ transferred to a company in the U.S., or if the company in the U.S. has voluntarily chosen the EU DPAs as its independent recourse mechanism, an informal panel of several EU DPAs will be set up to handle the complaint.

The informal panel of EU DPAs will launch an investigation during which both you and the company in the U.S. will have the possibility to express your views. If necessary in order to resolve the case, the informal panel can issue an 'advice', which is binding on the company in the U.S.

2.- Referral to U.S. authorities

If your complaint does not concern the processing of HR Data or the company in the U.S. has not committed to cooperate with the EU DPAs, the informal panel of EU DPAs will not be competent. Your national DPA may then refer your complaint to the competent U.S. authorities, such as the Federal

⁷ The terms "national data protection authority" or "EU handling authority" include the data protection authorities of the EEA and also the EDPS, which will be the EU handling authority when your personal data have been transferred to the U.S. by an EU institution.

⁸<https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization%E2%80%99s-Compliance-with-the-DPF-Principles>

⁹ <https://www.dataprivacyframework.gov/list>

¹⁰ Under the name of the company, click on "Full Profile" and go to "Dispute Resolution".

¹¹https://www.edpb.europa.eu/system/files/2024-04/dpf_template-complaint-form_commercial-complaints_en.pdf

¹² As for complaints regarding access to your personal data by U.S. national security authorities, please check the EDPB Information Note: https://www.edpb.europa.eu/system/files/2024-04/edpb_information-note_dpf-redress-mechanism-national-security-purposes_en.pdf

¹³ See definition of HR Data in Q1 above.

Trade Commission (FTC), the Department of Transportation's Office of Aviation Consumer Protection, or the U.S. Department of Commerce (DoC).¹⁴

Depending on the circumstances of the case, the national DPA which is competent for the EEA data exporter may also directly exercise its powers (such as prohibition or suspension of data transfers) towards the data exporter.

¹⁴ See decision on the adequacy of the Data Privacy Framework, Recitals 69, 80, and Annex V, Section II.A.