



EDPB Opinion

EU-US Data Privacy Framework (DPF)

Snapshot

March 2023

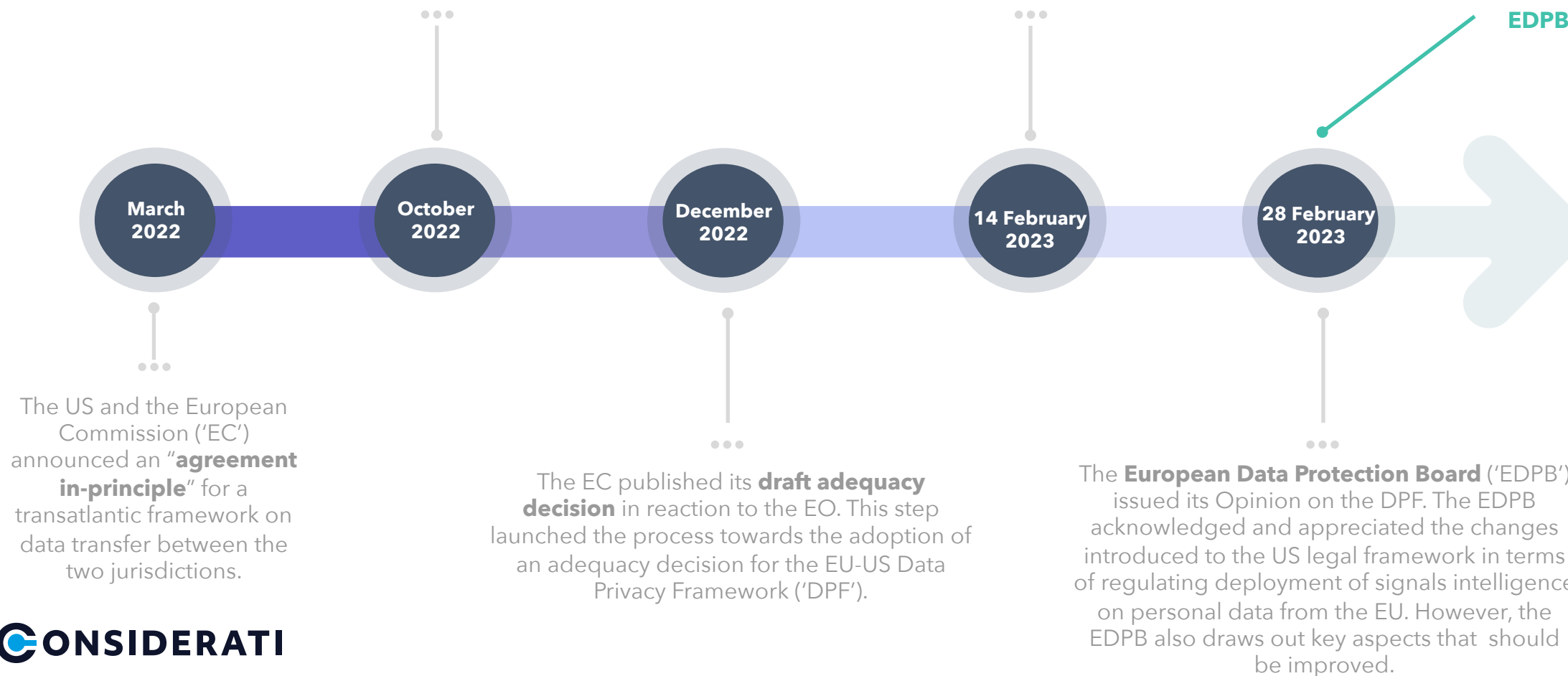
EU-US Data Privacy Framework Developments

US President Biden signed an **Executive Order** ('EO').

The EO put into practice the guarantees contemplated under the "agreement in-principle", particularly regarding safeguards against surveillance of personal data of EU residents by US intelligence agencies as well as protection of such data.

The **European Parliament** ('EP') released its draft resolution on the DPF urging the EC to not proceed. The EP held that the DPF's adequacy in affording equivalent protection to personal data as in the EU remains questionable.

Read the following slides for a snapshot of the latest development: the **EDPB Opinion**.



EDPB 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework'

"The EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain."

Overall, the EDPB positively notes the substantial improvements the EO offers compared to the previous legal framework (Privacy Shield), in particular the introduction of the principles of necessity and proportionality and the individual redress mechanism for EU data subjects.

However, given the concerns expressed and the clarifications required, the EDPB suggests these concerns should be addressed and that the European Commission provides the requested clarifications in order to solidify the grounds for the draft DPF. In addition, the EDPB recommends that the European Commission ensures close monitoring of the concrete implementation of this new DPF, in particular the safeguards it provides, in the future joint reviews.

Structure of EDPB Opinion



1. General Comments and Concerns

The EDPB expressed appreciation for:

- the international commitments and domestic legislative initiatives made by the US towards protection of fundamental rights including the right to privacy, as well as data protection;
- revision of the DPF principles to address the recommendations made by the CJEU in *Schrems II*.

The EDPB expressed concerns over:

- the need for more information on the legal context in the US that concerns and impacts the DPF;
- the largely unchanged principles in the DPF from the principles under the invalidated Privacy Shield.

The EDPB recommends that the EC make changes to:

- further clarify the scope of exemptions for use of signals intelligence under US laws in the DPF as well as the applicable safeguards under US law;
- be more closely informed of and monitor the application and adoption of any statute or government regulation that would affect adherence to the DPF Principles in the US;
- further improve the structure of the DPF and its annexes, ensure use of consistent terminology, and inclusion of definitions for some essential terms such as 'agent' and 'processor'.

2. General Data Protection Aspects

EDPB Observations and Recommendations

At the outset, the EDPB has reaffirmed that for a legal framework to be deemed “adequate” under Article 45 GDPR, it does not have to be identical to EU law, instead it must be evaluated if the data protection safeguards applicable to a data processing cycle are adequate in their entirety. In this light, the EDPB has made certain observations on the DPF’s alignment with the data protection principles envisioned under the GDPR. We have summed up a number of those observations below:

Purpose Limitation

- The DPF consists of terms such as ‘different purposes’, ‘materially different’ purposes, or ‘a use that is not consistent with’, but does not define these terms clearly. The EDPB opined that this could lead to legal uncertainty.

Data Subject Rights

- The Access principle addressing the data subjects’ rights to access, rectification and erasure under the DPF, is largely similar to the one contained in the annulled Privacy Shield, and thus entails the same issues as highlighted in the [WP29 Opinion 01/2016](#). For instance, certain exceptions to the right of access favour the DPF organisations without any requirement for considering the data subjects’ rights and interests. Similarly, the exception to the right of access for publicly available information and information from public records is quite broad, according to the EDPB.
- Modalities such as timing etc. for exercise of right to object are not specified in the DPF. EDPB has sought further clarification from the EC in this regard. Moreover, the EDPB has suggested that DPF should contain a general right to object if data subject(s) have legitimate grounds for their objection.

2. General Data Protection Aspects

EDPB Observations and Recommendations

Automated Decision Making and Profiling

- The DPF does not contain specific protection for individuals who are subjected to decisions solely based on automated processing of data, wherein such decisions are capable of having serious legal effects for individuals, for example in evaluating their performance at work, creditworthiness, reliability or conduct.
- The EDPB recommends including specific rules concerning automated decision-making in the DPF to provide sufficient safeguards, including by way of human oversight.
- The EDPB also noted that the existing safeguards against automated-decision making under US laws are varied and sector-specific, and thus possibly exclude certain situations and individuals.

Procedural and Enforcement Mechanisms

- Taking note of the fact that, like the Privacy Shield, the DPF relies on a self-certification mechanism, the EDPB has underlined the need for effective oversight for the enforcement of DPF and has stated that it will closely monitor the procedural and enforcement aspects of the DPF.

Redress Mechanism

- Given the similarity of the redressal mechanism to that under the erstwhile Privacy shield, the EDPB has sought clarity on the scope of EU Data Protection Authorities' (DPAs) advisory powers, as well as the weightage given to action taken by DPAs in enforcement proceedings.

3. Access and Use of Personal Data Transferred from the EU by Public Authorities in the US

EDPB Observations and Recommendations

Part 1: Access and Use of Personal Data for Criminal Law Enforcement Purposes

- The EDPB notes the more detailed assessment contained in the draft DPF compared to the previous Privacy Shield as far as access by federal law enforcement authorities is concerned. As for access by state law enforcement authorities, the EDPB also takes note that according to Annex VI of the draft DPF, state law protections must be at least equal to those of the US Constitution, including but not limited to the Fourth Amendment. The EDPB invites the EC to further assess the element of protections offered under state laws in the future reviews.
- The EDPB notes that the system of investigative tools used to obtain commercial data and other record information from corporations in the US for criminal law enforcement or public interest purposes – including the access limitations and safeguards – provides a comprehensive but also a complex system of measures, reflecting, among other things, the federal nature of the US government. The system of law enforcement investigative measures in the US could be considered as generally meeting the requirements of necessity and proportionality in relation to the fundamental rights to private life and data protection.
- The EDPB welcomes the clarifications provided by the EC as to the number of legal avenues for redress for individuals to rely on. The EDPB does invite the EC to further clarify whether these remedies allow the data subject to 'have access to personal data relating to him, or to obtain the rectification or erasure of such data' as required by the CJEU. Lastly, the EDPB holds that the EC should clarify the principles and safeguards applicable to further use of personal data within and outside of the US.

3. Access and Use of Personal Data Transferred from the EU by Public Authorities in the US

EDPB Observations and Recommendations

Part 2: Access and Use of Personal Data for National Security Purposes

- The EDPB, in its assessment of the protection offered by the DPF and the EO against the access and use of personal data for national security purposes by the US intelligence agencies, has recalled the importance of referring to the European Essential Guarantees on Surveillance Measures as a benchmark. Noteworthy guarantees include:

Guarantee A - Processing should be based on clear, precise and accessible rules

Requirements prescribed under the EO must be translated into practice by enacting and updating policies and procedures. The adoption of the DPF should be subject to such updates being made, and the EC must assess the updated policies and share its assessment with the EDPB.

Guarantee B - Demonstrable necessity and proportionate for legitimate objectives

The EDPB has sought clarity and more information on the various mechanisms under which personal data can be accessed for national security purposes, particularly under section 702 of Foreign Intelligence Surveillance Act ('FISA') and Executive Order 12333.

Further, with regard to the necessity and proportionality of bulk collection of data, the EDPB has observed that the EO continues to allow for indiscriminate collection of bulk data without sufficient safeguards, which is a matter of concern.

Guarantee C - Oversight

The EDPB generally observed that there exist sufficient internal oversight mechanisms for regulating signals intelligence activities.

For external oversight, while the EDPB welcomed the Privacy and Civil Liberties Oversight Board ('PCLOB'), it expressed concerns that EO does not improve the insufficiency of external oversight by the Foreign Intelligence Surveillance Court ('FISC') over the targeting of "non-U.S. persons".

Guarantee D - Availability of effective remedies

Among other aspects, the EDPB expressed concerns regarding the blanket "standard response" mechanism envisioned for the Data Protection Review Court ('DPRC'). Relying on decisions of the CJEU and the ECHR, and in light of the fact that the decisions of the DPRC are final, the EDPB has flagged this to be a point of review for the EC if the DPF were to be adopted.

Looking for guidance?

For over 15 years, Considerati has been the partner for the digital world

*We help
organisations to
innovate responsibly
with digital
technologies and data*

Legal

for compliance with privacy and data (related) regulations

Public Affairs

for societal and political support for technology & innovations

Responsible Tech

for an ethical compass when innovating with data & algorithms



Fitting technology into society

Our offices

Amsterdam

De Boelelaan 7

Den Haag

Anna van Buerenstraat 41 4DE

Contact information

+31 20 737 0069

info@considerati.com

www.considerati.com