



WILSON
SONSINI

Latest Developments on the EU-U.S. Data Privacy Framework

May 10, 2023

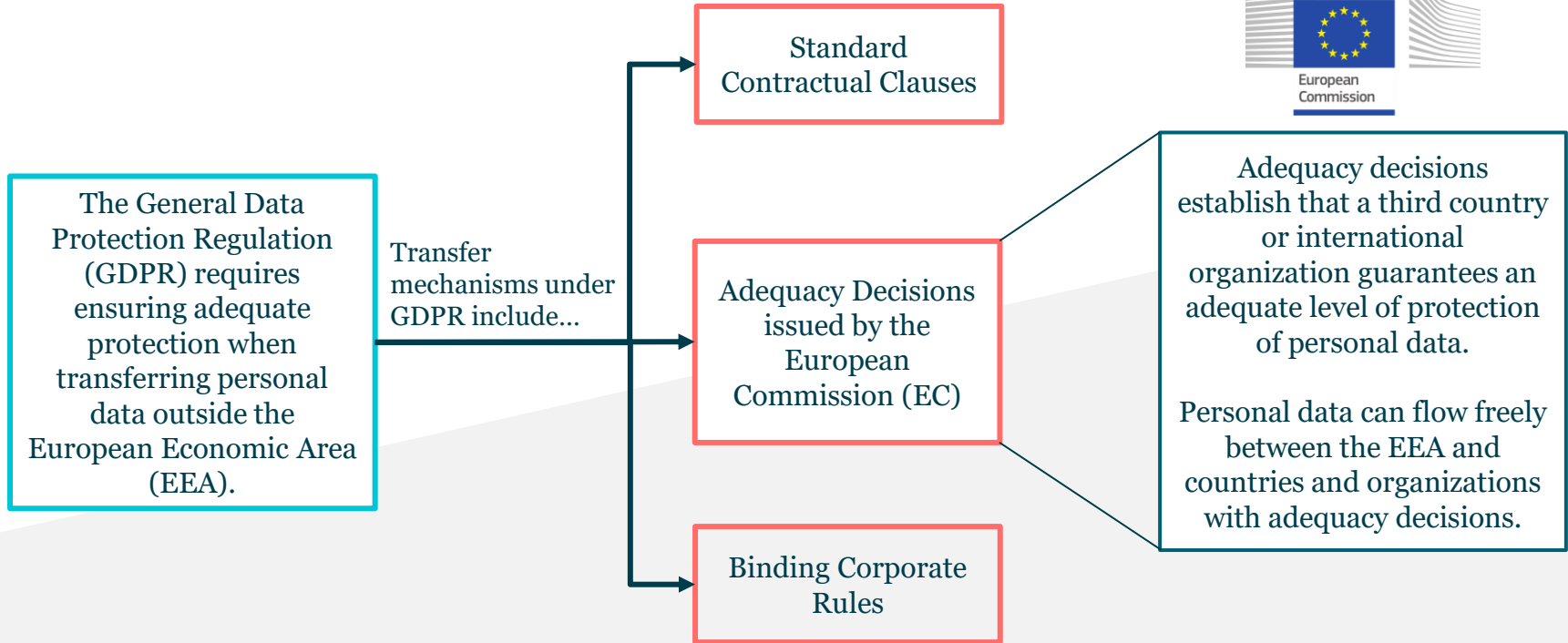
Agenda

- 1. *Background***
- 2. *Practical aspects of certification***
- 3. *What's next***
- 4. *Questions***

Background

**WILSON
SONSINI**

Background: International Data Transfers



Background: International Data Transfers (Cont'd)

Thousands of U.S. companies relied on Privacy Shield

- Over 5,000 U.S. companies relied on the Privacy Shield adequacy decision for transfers, until the Court of Justice of the EU (CJEU) invalidated it in 2020 in the “*Schrems II*” case.



Schrems II invalidated the Privacy Shield in July 2020

Main reasons for invalidation:

- Lack of adequate protection to individuals’ data protection rights in light of potential for broad disclosures of personal data to U.S. intelligence services/public authorities; and
- Lack of a suitable judicial redress mechanism for individuals in the EU whose personal data was transferred to the U.S.



New transfer framework negotiated

- Since then, the EU and the U.S. have been working on creating a new data transfer framework. The negotiations have been complex and politically sensitive.



Key steps of the process so far

- **March 25, 2022** - President von der Leyen and President Biden announced an agreement in principle on a new EU-U.S. Data Privacy Framework.
- **October 7, 2022** - President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities.
- **December 13, 2022** - European Commission published a draft adequacy decision on the level of protection of personal data under the EU-U.S. Data Privacy Framework.
- **February 28, 2023** - EDPB adopted opinion on draft adequacy decision; called for clarifications on several points.



In the meantime...

Some companies remain Privacy Shield certified (and implemented SCCs).



New definition for “data transfer”: B2C companies in the U.S. may not even need a data transfer mechanism when collecting personal data directly from their users in the EU.



Companies using SCCs often struggle with the new obligation to carry out Data Transfer Impact Assessments (DTIAs).



Data flows to the U.S. are under scrutiny from Supervisory Authorities.



Practical aspects of certification

What will the EU-U.S. Data Privacy Framework mean for businesses?

Free-flow of personal data

- Once finalized, certified companies will be able to freely import personal data from the EU into the U.S. without the need to rely on another data transfer mechanism, such as SCCs.

Begin preparations

- At this stage, businesses must continue to rely on alternative data transfer mechanisms for data transfers, but can begin to prepare for the process to certify to the new framework.

EC published draft decision in December 2022

- Draft adequacy decision, released by the EC in December 2022, assesses how the Data Privacy Framework satisfies the requirements of the GDPR and the *Schrems II* ruling, and outlines requirements for organizations participating in the Data Privacy Framework.



Brussels, XXX
[...](2022) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

(Text with EEA relevance)

EN

EN

Overview

Public Commitment to Principles



- Companies must publicly disclose commitments to comply with the EU-U.S. Data Privacy Framework (DPF) Principles.



- Principles keep the same headings as under Privacy Shield.
- The substance of some of the supplemental principles has been slightly altered

Voluntary Self-Certification



- Voluntary self-certification mechanism, subject to annual review.

Enforced by the FTC (or DoT)



- The Federal Trade Commission will ensure companies comply with the Data Privacy Framework Principles.



- Department of Commerce maintains a list of certified companies and a list of formerly certified companies (together with reasons for removal).

The EU-U.S. Data Privacy Framework (“DPF”) Principles

7 Principles:

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability

Complemented by 16 Supplemental Principles:

1. Sensitive data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of Data Protection Authorities
6. Self-Certification
7. Verification
8. Access
9. HR Data
10. Obligatory Contracts for Onward Transfers
11. Dispute Resolution and Enforcement
12. Choice – Timing of Opt-Out
13. Travel Information
14. Pharmaceutical and Medical Products
15. Public Record and Publicly Available Information
16. Access Requests by Public Authorities

1. Notice

Elements to include in privacy notice (either as part of general privacy notice or specific DPF notice):

1. Participation in the DPF and link to the DPF list;
2. Types of personal data collected and the affiliates adhering to the DPF;
3. Commitment to subject to the DPF all EU personal data received in reliance on the DPF;
4. Purposes for which it collects and uses personal data;
5. Contact details for inquiries and complaints;
6. Categories or identity of data recipients and purposes of data disclosures;
7. Individuals' right of access;
8. Individuals' choices and means the organization offers individuals for limiting the use and disclosure of their personal data;
9. Independent dispute resolution body;
10. Confirmation of FTC / DoT jurisdiction;
11. Possibility for individuals to invoke binding arbitration;
12. Requirement to disclose personal data to lawful public authorities' requests; and
13. Liability in case of onward transfers to third parties.



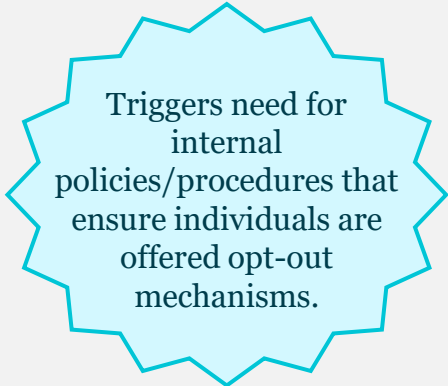
2. Choice

Organizations must offer:

- Opt-out via a clear, conspicuous and readily available mechanism in 2 situations:
 - Data is disclosed to a third party acting as a controller.
 - Data is to be used for a purpose that is materially different from the purpose of collection.
- Opt-out is not required when data is disclosed to agents (processors).
- Affirmative express consent (opt-in) is required for sensitive data.
- Opt-out from marketing communications.

EU Commission's Guide to the Privacy Shield (same requirements as under DPF):

- Use for incompatible purpose is not permitted.
- Choice principle applies to use for a new purpose that is different but related to the original one (i.e., materially different).



Triggers need for internal policies/procedures that ensure individuals are offered opt-out mechanisms.

3. Accountability for Onward Transfer: to a third-party controller


- Comply with Notice and Choice Principles (i.e., provide notice & opt-out); and
- Conclude agreement requiring the third party controller to:
 - Process data for limited and specific purposes consistent with the purpose of collection; and
 - Protect the data with the same level of protection as provided by the DPF Principles.
 - Notify the DPF company if it cannot meet the latter obligation, and stop processing or take steps to remediate.
- However, the third party controller does not need to be DPF-certified and to have an independent recourse mechanism, provided that a similar mechanism is available.
- For data transfers within the same corporate group, possibility to rely on other data transfer mechanisms (such as BCRs, Intra-Group Agreement) instead of the above agreement.



Triggers need to review third party contracts.

3. Accountability for Onward Transfer: to a third-party agent (processor)

- Only transfer data for limited and specified purposes;
- Conclude agreement to:
 - Ascertain that the agent is obligated to provide at least the same level of protection.
 - Require the agent to notify when it cannot meet the latter obligation.
- Ensure agent uses data in a manner consistent with companies' obligations under the Principles.
- Upon notice, take steps to stop and remediate unauthorized processing.
- Upon request, provide a copy/summary of data processor agreement to DoC.
- Companies are liable for non-compliance by agent, unless they prove that they are not responsible for event giving rise to damage.




Triggers need to review third party contracts.

4. Security

Threshold for security measures, similar to GDPR.


- Companies must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction; and take into due account the risks involved in the processing and the nature of the personal data.
- Similar to security requirements of GDPR.



Triggers need to review data security policies / procedures.

5. Data Integrity and Purpose Limitation

- Data integrity: data must be reliable for its intended use, accurate, complete and current.
- Purpose limitation: obligation to limit the data to what is relevant for the purpose of processing.
- Data retention: information may be retained in a form identifying or making identifiable the individual only for as long as it serves the purpose of the collection.
- A company must protect the data in accordance with the Principles for as long as it retains the data.



Triggers need for
internal data handling
and retention
policies/procedures.

6. Access

Individuals must have access to personal data and be able to correct, amend, or delete it when it is inaccurate, or when it has been processed in violation of the Principles.

Close to EU data protection law:

- Confirmation of whether the organization is processing personal data, including information on the categories of data, purpose of processing and categories of recipients.
- Communicate the data so that individuals can verify its accuracy and lawfulness.
- Have data corrected, amended or deleted where it is inaccurate, outdated, or processed in violation of the Principles.

Modalities:

- Individuals do not have to justify requests for access to the company (unless request too broad or vague).
- Obligation to make good faith efforts to comply with individuals' access requests.
- Timeframe (reasonable time period).
- Format (in a reasonable manner, and in a form that is readily intelligible to the individual).
- Possibility to charge fees (not excessive).
- Any denial of, or limitation to the right of access has to be necessary and duly justified.

6. Access (Cont'd)

Exceptions:

- Burden or expense of providing access would be disproportionate.
- Confidential commercial information.
- Violation of third parties' rights.
- Breach of a legal or other professional obligation; prejudicing employee security investigations.
- Confidentiality requirements.
- Conflict with legal obligations.

7. Recourse, Enforcement and Liability

1. Verification mechanism: self-assessment or outside compliance review.

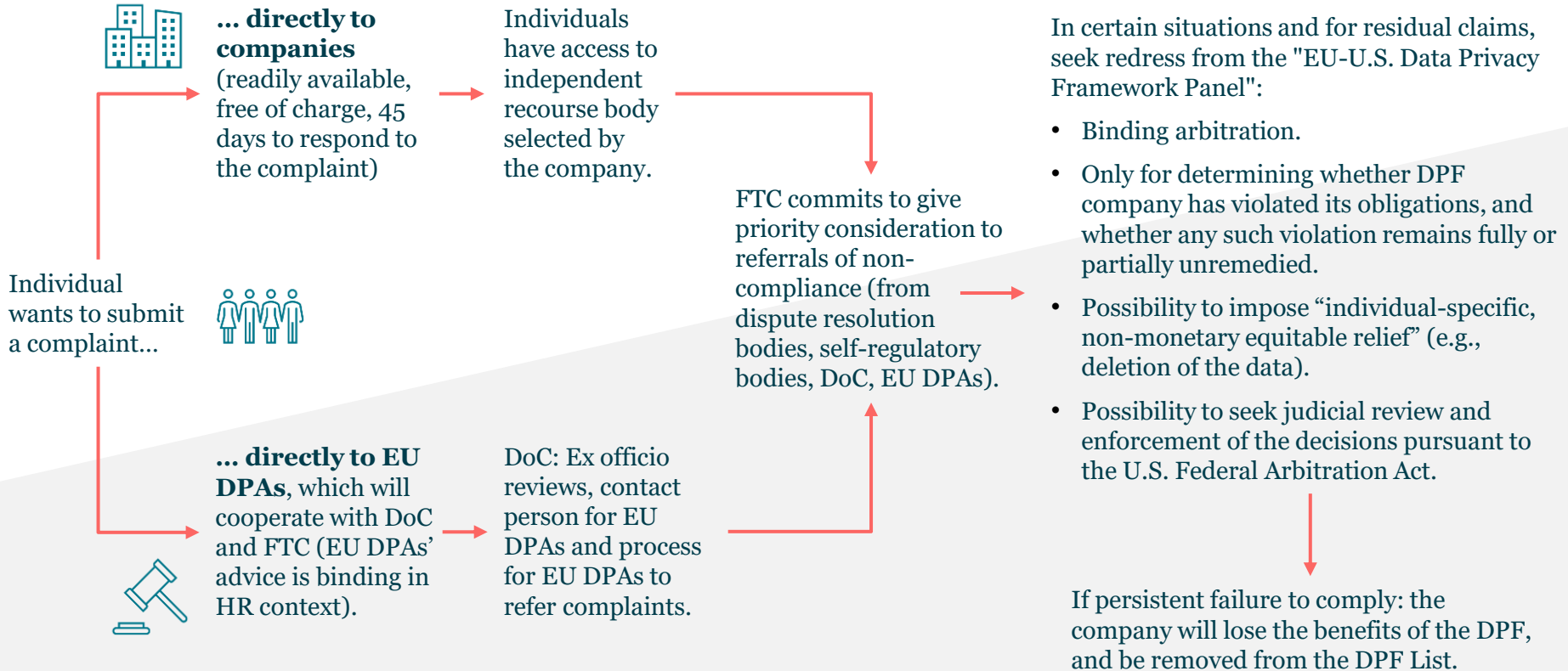
- Content is specified (conformity of the privacy policy, information re: the complaint handling procedure, training and disciplinary sanctions, periodical objective reviews, signed by a corporate officer).
- Outside compliance can be auditing, random reviews, use of “decoys” or technology tools.
- Obligation to maintain records on the implementation of DPF privacy practices.

2. Independent recourse mechanism:

- 3 ways to satisfy the requirements: (i) private sector privacy programs with effective enforcement mechanism; (ii) compliance with legal or regulatory supervisory authorities; or (iii) commitment to cooperate with EU DPAs.
- Must be readily available, at no cost for the individuals, and expeditiously resolved.
- Selected by the company prior to self-certifying.
- Remedies: non-compliance is reversed, compliance of future processing and stop the violation.
 - Including publicity for findings of non-compliance, deletion of data, compensation for individuals.
- Failure to comply with ruling of dispute resolution body must be notified to the DoC and the FTC / DoT / Courts.
- Organization and their independent recourse mechanism must respond promptly to DoC requests and to complaints referred by EU DPAs via the DoC.
- Privacy notice must include information about independent dispute resolution body.

3. Obligation to remedy problems arising out of non-compliance.

Complaints Handling: Overview



Monitoring, Periodic Joint Review and Suspension

EU Commission has obligations to monitor the DPF:

- Periodic factual & legal checks.
- Continuous monitoring of the overall functioning of the DPF, and compliance by U.S. authorities with their representations and commitments.

The EU and the U.S. will conduct a periodic joint review:

- Covering the functioning of all aspects of the DPF, including national security, and involving all relevant stakeholders (e.g., U.S. national intelligence experts, EU DPAs, NGOs through the participation at a public conference).
- Taking into account the U.S. government commitments and transparency reports published (voluntarily) by companies.
- The result will be presented to EU Parliament and Council of the EU.

If the U.S. does not fulfill its commitments, the DPF may be suspended by EU Commission.

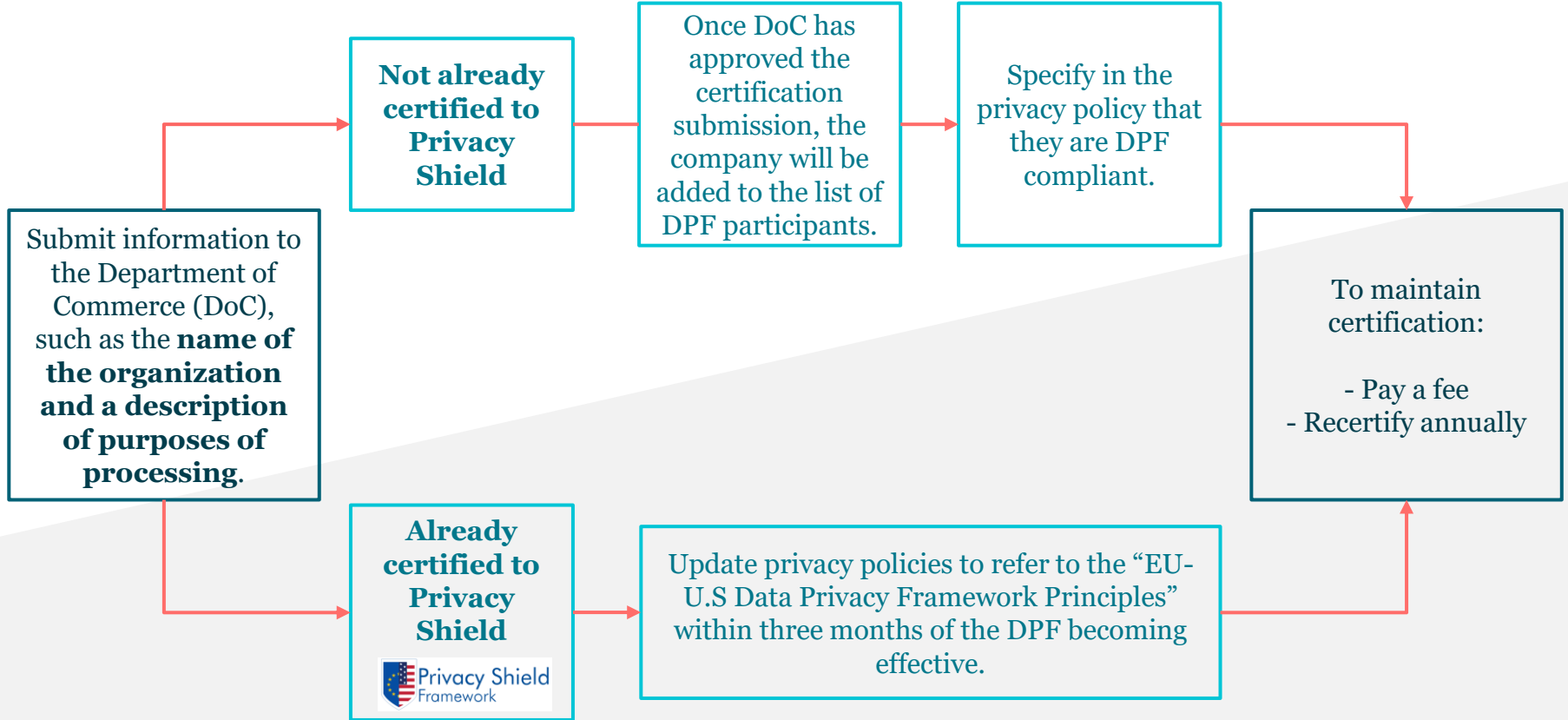
Processing for National Security Purposes

Two main differences between the Privacy Shield and the DPF in this area:

1. U.S. intelligence agencies will only access European data to the extent such access is **necessary and proportionate** to protect national security.
2. The Privacy Shield Ombudsperson, an official charged with reviewing queries from European citizens regarding U.S. intelligence authorities' access to personal data, has been replaced with a newly created **Data Protection Review Court**, which will independently investigate complaints from European citizens, offering an avenue for redress.



How to get certified



What's next

WILSON
SONSINI

European Parliament Committee issues negative draft opinion

- The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) said that the EC should not give the U.S. adequacy status based on the DPF
- Found that the framework does not create actual equivalence of data protection. For example:
 - The Data Protection Review Court is part of the executive branch and not the judiciary;
 - Other countries that have received adequacy decisions have national data protection laws, whereas the U.S. does not;
 - Remedies available for commercial matters are insufficient and these issues are largely left to the discretion of companies.
- Called for meaningful reforms to take place.
- LIBE previously issued a (similarly nonbinding) resolution in 2018 calling for the Privacy Shield to be invalidated. However, the EC stood behind the Privacy Shield in the face of this criticism.

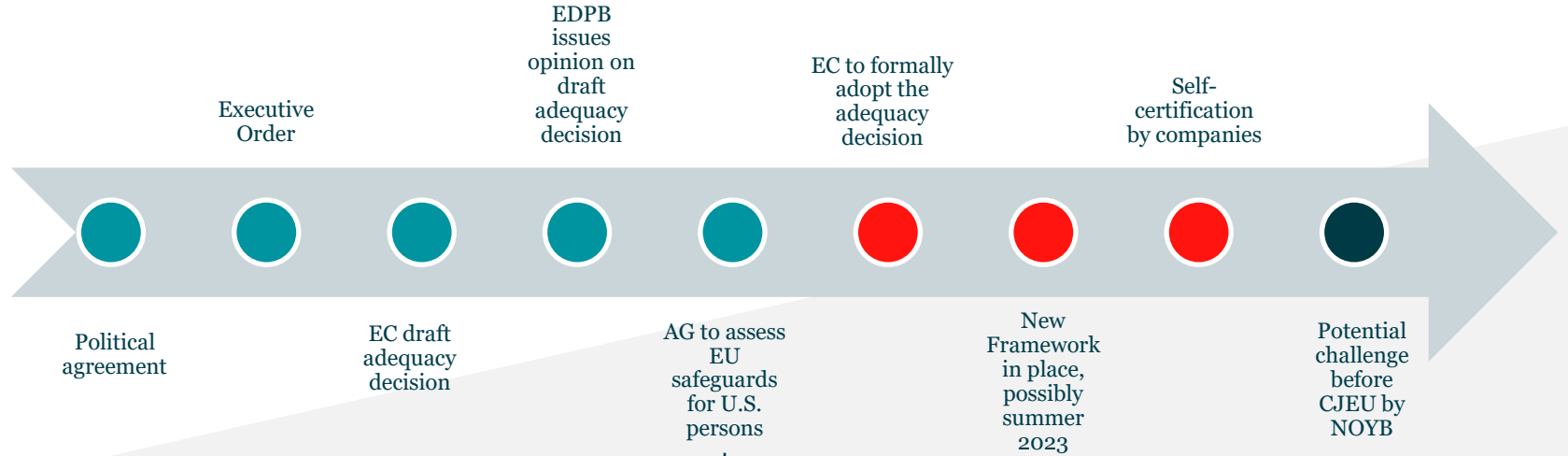


European Data Protection Board (“EDPB”) issues mixed opinion

- While not binding, the EDPB’s opinion carries considerable political and legal weight, and has forced rewrites in the past
- Positively notes:
 - The introduction of the principles of necessity and proportionality
 - The individual redress mechanism for EU citizens, in particular the Data Protection Review Court
 - Commitment by U.S. authorities to enforce the DPF
- But criticizes:
 - Exceptions to the right to access may be too broad
 - Lack of clarity around how the principles apply to processors
 - Overly broad "publicly available information" exemption
 - Lack of specific rules on automated decision-making and profiling
 - Lack of safeguards for onward transfers of personal data
 - No requirement for prior authorization by an independent authority for bulk collection of data



Next Steps for the New EU-U.S. Data Privacy Framework



- The U.S. Attorney General will assess whether EU member states offer appropriate reciprocal safeguards regarding their own signals intelligence on the personal data of U.S. persons
- The AG will then designate the EU as a “qualifying regional economic integration organization”.

Schrems III...?

- Austrian privacy advocate, Max Schrems, has already signaled that he plans to challenge the validity of the decision, given that it is based on the Executive Order which he believes will not satisfy the CJEU.
- For instance, Schrems believes that:
 - The proposed Data Protection Review Court is not an actual court and it will not offer sufficient redress for European citizens.
 - Continuous “bulk surveillance” of European citizens will remain.

noyb

News Projects Resources Support us! About us EN Q

HOME > NEWS > STATEMENT ON EU COMMISSION ADEQUACY DECISION ON US

Statement on EU Commission adequacy decision on US

Dec 13, 2022

Project

[EU-US Data Transfers](#)

Support us!

noyb funding goal

74 %

INVEST IN PRIVACY!

Follow us!

[f](#) [t](#) [v](#) [in](#)

[e](#) [m](#) [s](#)

Media Coverage

THE IRISH TIMES

DPC seeking penalty of up to €36m against Facebook

The Data Protection Commission (DPC) has suggested a penalty of between €28 million and €36 million for Facebook in a draft decision made against the company.

Austrian privacy and data rights campaigner Max Schrems's NOYB organisation, which filed the original complaint against the technology giant, has published the commission's draft decision online.

[Read More](#)

Statement on US Adequacy Decision by the European Commission

Today, the European Commission issued a new adequacy decision replacing the "Privacy Shield" decision, that was previously invalidated by the Court of Justice of the EU (CJEU) over US surveillance. The CJEU required (1) that US surveillance is proportionate within the meaning of Article 52 of the Charter of Fundamental Rights (CFR) and (2) that there is access to judicial redress, as required under Article 47 CFR. Updated US law (Executive Order 14086) seems to fail on both requirements, as it does not change the situation from the previously applicable PPD-28. There is continuous "bulk surveillance" and a "court" that is not an actual court. Therefore, any EU "adequacy decision" that is based on Executive Order 14086 will likely not satisfy the CJEU.

- [EU Commission adequacy decision on US](#)
- [New Executive Order 14086](#)
- [Previous Executive Order of 2014 \(PPD-28\)](#)
- [noyb statement on the Executive Order](#)

Potential UK Framework

- There has been no formal reaction to the draft adequacy decision from the UK Government.
- However, the UK Government welcomed the signing of the Executive Order and has expressed its intent to qualify as a regional economic integration organization.


Department
for Culture,
Media & Sport


Department for
Digital, Culture,
Media & Sport

Guidance

UK-US Joint Statement: New Comprehensive Dialogue on Technology and Data and Progress on Data Adequacy

Published 7 October 2022



Impact on other data transfer mechanisms

- *Schrems II*: organizations that transfer personal data outside the EU must carry out a “Data Transfer Impact Assessment” (“DTIA”), unless they rely on an adequacy decision.
- Can organizations using SCCs to transfer personal data to the US invoke the changes to US law (brought by the DPF) to come to a more favorable outcome in their DTIA?

Questions?

WILSON
SONSINI

Thank you

WILSON
SONSINI

