Published on 30 August 2023 by **Claire Filliatre**, Member of the Lyon Bar
c.filliatre@soulier-avocats.com
Tel.: +33 (0)4 72 82 20 80

Read this post online

European Union adopts a new framework for the transfer of personal data to the USA

On July 10, 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.

This decision concludes that the USA ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the European Union to U.S. companies under the new Framework.

As such, personal data can henceforth flow safely from the European Union to U.S. companies adhering to the new Framework, without having to put in place additional data protection safeguards.

The adequacy decision[1] adopted by the European Commission follows the signature in the USA of an Executive Order which introduced new binding safeguards to address all the concerns raised by the Court of Justice of the European Union ("CJEU"), including limiting access to EU data by U.S. intelligence services to what is "*necessary*" and "*proportionate*", and establishing a Data Protection Review Court.

European Commission President Ursula von der Leyen welcomed the adoption of this long-awaited decision, saying:

> *"The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the U.S. has implemented unprecedented commitments to*

establish the new framework. Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the U.S., and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues."

Background

Article 45(3) of the General Data Protection Regulation ("GDPR")[2] grants the European Commission the power to decide, by means of an implementing act, that a non-EU country ensures "*an adequate level of protection*", i.e., a level of protection for personal data that is essentially equivalent to the level of protection within the European Union.

An adequacy decision is one of the tools provided under the GDPR to transfer personal data from the EU to third countries which, in the assessment of the European Commission, offer a comparable level of protection of personal data to that of the EU.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area[3] to a third country, without being subject to any further conditions or authorizations.

After the invalidation of the previous adequacy decision on the EU-U.S. Privacy Shield by the CJEU in its "Schrems II" decision of July 2020[4], the European Commission and the U.S. Government entered into discussions on a new framework that would address the issues raised by the CJEU.

In March 2022, European Commission President von der Leyen and President Biden announced that they had reached an agreement in principle on a new transatlantic data flows framework[5].

In October 2022, President Biden signed an Executive Order on "*Enhancing Safeguards for United States Signals Intelligence Activities*"[6], which was complemented by regulations issued by U.S. Attorney General. These elements implemented the U.S. commitments reached under the agreement in principle into U.S. law, and complemented the obligations for U.S. companies under the new EU-U.S. Data Privacy Framework.

The new EU-U.S. Data Privacy Framework

The EU-U.S. Data Privacy Framework ("DPF") provides EU individuals whose data are transferred to adhering organizations in the USA with several new rights (e.g., obtaining access to their data, obtaining the correction or deletion of incorrect or unlawfully handled data, etc.).

EU individuals will also benefit from several redress avenues in case their data is wrongly handled by U.S. organizations. This includes free of charge independent dispute resolution mechanisms and an arbitration panel (see below).

U.S. organizations can certify their participation in the DPF by committing to comply with a detailed set of

privacy obligations such as, for example, purpose limitation, data minimization and data retention, as well as specific obligations concerning data security and the sharing of data with third parties (together referred to officially as the "Principles").

The DPF will be administered by the U.S. Department of Commerce, which will process U.S. organizations' applications for certification and monitor whether adhering organizations continue to meet the certification requirements.

Compliance by U.S. organizations with the Principles and their obligations under the DPF will be enforced by the U.S. Federal Trade Commission.

The International Trade Administration of the U.S. Department of Commerce has created a website to help U.S. organizations understand the benefits and requirements of adhering to the DPF[7]. This website also contains an up-to-date list of adhering U.S. organizations.

Limitations and safeguards regarding access to data by United States intelligence agencies

In its "Schrems II" decision, the CJEU had pointed out that U.S. domestic regulations implied significant limitations to the protection of personal data, justified *inter alia* by public security, defense and national security interests – in particular to allow the implementation of certain surveillance programs.

It considered that this type of limitations, and the interference that they entailed with the fundamental rights of the persons whose data are transferred, were not sufficiently regulated in the light of the rules of the EU.

It also considered that the ombudsperson mechanism provided for under the former EU-U.S. Privacy Shield did not constitute a remedy offering guarantees equivalent to those offered in the European Union, namely the independence of the body before which complaints were brought and the binding nature of the decisions issued by that body.

The U.S. Executive Order on "*Enhancing Safeguards for United States Signals Intelligence Activities*" and related regulations issued by U.S. Attorney General were designed to address these concerns.

Specifically, for EU individuals whose personal data is transferred to the U.S.A., the new U.S. legislation provides for:

- Binding safeguards that limit access to data by U.S. intelligence authorities to what is "*necessary*" and "*proportionate*" to protect national security;
- Enhanced oversight of activities by U.S. intelligence services to ensure compliance with limitations on surveillance activities; and
- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to transferred data by

U.S. national security authorities.

The new redress mechanism regarding access to transferred data by U.S. national security authorities

EU individuals will have access to an independent and impartial redress mechanism regarding the collection and use of their data by U.S. intelligence agencies.

The U.S. Government has established a new two-layer redress mechanism, with independent and binding authority.

For a complaint to be admissible, individuals do not need to demonstrate that their data was actually collected by U.S. intelligence agencies. They can submit a complaint, in their own language, to their national data protection authority that will be responsible for ensuring that the complaint will be properly transmitted and that any further information concerning the procedure and the outcome of the complaint will be provided to the relevant individual.

Complaints will be transmitted to the U.S.A. by the European Data Protection Board.

The process will be as follows:

Firstly, complaints will be investigated by the so-called "*Civil Liberties Protection Officer*" of the U.S. intelligence community. The Civil Liberties Protection Officer, who is responsible for ensuring compliance by U.S. intelligence agencies with privacy and fundamental rights, will issue a decision.

Secondly, individuals have the possibility to appeal the decision of the Civil Liberties Protection Officer before the newly created Data Protection Review Court ("DPRC"). The DPRC is composed of members from outside the U.S. Government who are appointed on the basis of specific qualifications and who can only be dismissed for cause. The DPRC has powers to investigate complaints from EU individuals to obtain relevant information from intelligence agencies, and can take binding remedial decisions.

In each case, the DPRC will select a special advocate with relevant experience to ensure that the complainant's interests are represented and that the DPRC is well informed of all factual and legal aspects of the case.

Redress in case of non-compliance with the Principles

The adequacy decision provides EU individuals with a number of possibilities to enforce their rights in case organizations adhering to the DPF not comply with the Principles.

Data subjects can, as the case may be, bring a complaint directly to an organization adhering to the DPF, to an independent dispute resolution body designated by said organization, to national data protection authorities, to the U.S. Department of Commerce or to the U.S. Federal Trade Commission.

It is interesting to note that any organizations adhering to the DPF must put in place an effective redress mechanism to deal with such complaints. Their privacy policy must, therefore, clearly inform individuals about a contact point, either within or outside the organization, that will handle complaints, as well as about the designated independent dispute resolution body. The organization must provide a response to the data subject within a period of 45 days from receipt of the complaint.

Data subjects can also bring a complaint directly to the independent dispute resolution body (either in the EU or in the United States) designated by the organization adhering to the DPF. This recourse is free of charge to the relevant individual.

If they so wish, data subjects may equally bring their complaints to a national data protection authority in the EU. Organizations adhering to the DPF shall be obliged to cooperate with the data protection authority either when (i) the complaint concerns the processing of human resources data collected in the context of an employment relationship, or (ii) when the relevant organization has voluntarily submitted to the oversight by EU data protection authorities.

In some cases, EU national data protection authorities may forward the complaints received to the U.S. Department of Commerce that has committed under the adequacy decision to examine it and make its best efforts to deal with it.

Lastly, the Federal Trade Commission, which has the necessary investigatory and enforcement powers, may be called upon to effectively ensure compliance with the Principles by organizations adhering to the DPF, mainly at the request of independent dispute resolution bodies, the U.S. Department of Commerce or EU national data protection authorities.

If none of the above redress avenues has satisfactorily resolved a complaint, the data subject may, as a recourse mechanism of "last resort", invoke binding arbitration by the "*EU-U.S. Data Privacy Framework Panel*".

This panel shall consist of a pool of at least ten arbitrators that will be designated by the U.S. Department of Commerce and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties select from this pool a panel of one or three arbitrators.

In addition, wherever an organization adhering to the DPF does not comply with its commitment to respect the Principles, data subjects may seek judicial redress in the USA to obtain compensation (e.g. under U.S. consumer laws, tort law, etc.)

Towards a "Schrems III" decision?

Despite efforts on both sides of the Atlantic in recent years to establish a new protection framework, the validity and effectiveness of the DPF are already much debated.

Opponents argue *inter alia* that the DPRC is in fact a body functioning within the executive branch of the U.S. Government and does not constitute in any way an "impartial tribunal" within the meaning of Article 47 of the EU Charter of Fundamental Rights[8].

Max Schrems, founder of the NGO None of your business ("NOYB"), believes that the new transatlantic data protection framework is a mere copy of the 2016 Privacy Shield, which was itself a copy of the 2000 Safe Harbor, and deplores the lack of substantial change in U.S. surveillance law.

He has already announced that he is ready to bring a case before the CJEU:

> *"NOYB has prepared various procedural options to bring the new deal back before the CJEU. We expect the new system to be implemented by the first companies within the next months, which will open the path towards a challenge by a person whose data is transferred under the new instrument. It is not unlikely that a challenge would reach the CJEU by the end of 2023 or beginning of 2024."*

---

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

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[3] The European Economic Area ("EEA") includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein.

[4] See *inter alia* our article entitled International data transfers to the USA: The Privacy Shield invalidated by the CJEU published on our Blo in August 2020

[5] See European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework dated March 25, 2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

[6] *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities* of October 7, 2022 available on the White House's website: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

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

[8] Article 47 of the EU Charter of Fundamental Rights stipulates as follows: *"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a*

tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice."