NEW EU-US DATA PRIVACY FRAMEWORK—RELIABLE SOLUTION FOR TRANSATLANTIC DATA TRANSFERS OR GATEWAY TO SCHREMS III?

Date: 12 July 2023

Data Protection, Privacy, and Security Alert

By: Dr. Thomas Nietsch, Whitney E. McCollum

IN A NUTSHELL

On 10 July 2023—nearly three years to the day after theSchrems II decision of the Court of Justice for the European Union (CJEU) (Schrems II Decision, see our Alert here)—the EU Commission has adopted the adequacy decision for the new and entirely revamped EU-US Data Privacy Framework (DPF) as a means to secure transfers of personal data from the European Union to companies in the United States. This decision is a separate tool for justification of data transfers under Chapter V of the General Data Protection Regulation (GDPR) and stands next to other established means, such as Standard Contractual Clauses, Binding Corporate Rules, or Codes of Conduct. The adoption decision will allow data transfers from the European Union (or by companies otherwise subject to the GDPR) to companies in the United States that have signed up to the DPF program and are thus required to meet certain data protection minimum standards. Compliance with these minimum standards is monitored by the US Department of Commerce and the US Federal Trade Commission. In addition to this, the United States has also committed to restrict access of administrative authorities to personal data subject to GDPR and now grant a right of redress to an independent court in case of violations of their privacy rights.

In July 2020, the CJEU annulled the predecessor of the DPF, the EU/US Privacy Shield, which did not, in the court's view, sufficiently take into account the broad investigation rights and practices by U.S. authorities, lacked oversight and redress mechanisms, and consequently attested a general lack of protection of personal data of EU citizens. Since this court decision, EU companies were struggling to find a way to engage with and lawfully transfer personal data to US-based companies, as therecommendations by the European Data Protection Board (EDPB) imposed quite onerous obligations on EU companies, narrowing the choices to using EU service providers or accepting substantial risks of non-compliance with GDPR.

The DPF is intended to put an end to this period of uncertainty and to provide for a reliable and practicable safeguard to transfer personal data to US-based companies.

THE STORY SO FAR

The GDPR requires exporters of personal data to ensure that any recipient of personal data outside the European Union maintains an “adequate” level of data protection (Art. 44 GDPR). This is because many companies not located in the European Union are not subject to the comprehensive data protection and privacy rules imposed by GDPR. “Adequate” protection can be achieved by several means expressly mentioned in Chapter V of the GDPR.

The broadest and most reliable tool is a so-called adequacy decision issued by the EU Commission, which recognizes that the privacy laws bearing on the data importer are subject provide for a substantially equivalent level of data protection and thus the personal data transferred from the European Union is safe in that destination. However, only a few countries so far benefit from such an adequacy decision. The United States is not among these countries, mainly because local laws neither provide for comprehensive privacy laws nor grant the same level of data protection to foreign citizens as to US citizens. In particular, a long-standing criticism of the US framework is since the Snowden revelations in 2013 related to the possibility for US administrative authorities to access personal data relating to non-US citizens in broad and basically unrestricted fashion.

While the lack of comprehensive privacy laws for private US entities could be overcome by their voluntary adherence to certain minimum data protection standards; the alleged excessive access by US authorities to foreign personal data required a political consensus between contrasting EU- and US-interests.

This was already the basic idea of the Safe Harbor framework, which wasinvalidated by the CJEU in 2015 (Schrems I) and also its successor, the EU/US Privacy Shield that was, in a landmark decision of the CJEU, also invalidated in 2020.

Such consensus was reached, from a political standpoint, in early 2022, where US President Joe Biden and EU Commission President Ursula von der Leyen surprisingly announced a principle understanding that led to the US Executive Order 14086 in October 2022, which forms the baseline of the DPF and the respective adequacy decision of the EU Commission.

On 28 February 2023, the EDPBissued an opinion on the draft adequacy decision of the EU Commission suggesting further improvements of the decision, before the final adequacy decision was issued on 10 July 2023.

WHAT DOES THE ADEQUACY DECISION REQUIRE FROM US ENTITIES?

Similar to what has already been established by the preceding Safe Harbor and the EU and US Privacy Shield programs, the key element of the DPF is the commitment of US entities wishing to participate in the DPF program to adhere to and self-certify under a set of privacy obligations, which reflect the core principles of GDPR and are issued by the US Department of Commerce (DoC). Consequently, only entities falling under the jurisdiction of the DoC are eligible for participation.

These core privacy principles include:

- Purpose limitation (similar toArt. 5(1) lit. b) GDPR);
- Special protection for 'special categories' of personal data (similar toArt. 9 GDPR);
- Data accuracy, minimization, and security (similar to Art. 5(1) lit. d), e) and f) GDPR);
- Transparency (similar to Art. 5(1) lit. a) andArt. 13, 14 GDPR);
- Individual rights (similar to Art. 15, 16, 17, 21 GDPR);
- Accountability for onward transfers (either within or outside the United States) under essentially the same principles as laid down above; and
- Accountability (similar to Art. 5(2) GDPR).

Compliance with these principles is monitored and enforced in case of breach by the DoC and Federal Trade Commission.

To ensure in particular effective enforcement of data subject claims, US entities under the DPF umbrella need to provide for an independent dispute resolution body either in the European Union (e.g. EU data protection authorities) or in the United States that provides for effective and binding remedies. Ultimately, if complaints do not prove effective in a certain case, the data subject is entitled to invoke a binding arbitral proceeding administered by theInternational Centre for Dispute Resolution of the American Arbitration Association.

WHAT DOES US EXECUTIVE ORDER 14086 SAY?

Executive Order 14086 complements the obligations of private entities and contains commitments by the US government to enhance the protection of personal data of EU citizens when processed by US authorities. These include in particular binding safeguards that restrict access to foreign data to the necessary and proportionate extent for national security. Any intelligence activity by the United States must be conducted pursuant to at least one of 12 legitimate objectives and done in a manner proportionate to the priority as compared with the risk to privacy rights. To ensure that EU citizens are awarded with an effective right of redress against handling of their personal data by US intelligence agencies, the United States established a two-layer protection mechanism:

- The first layer is the right of an EU citizen to complain if the personal data protected under GDPR has actually been accessed by a US intelligence agency. The complaint can be submitted to the national data protection supervisory authority in the EU member state of residence of the data subject and will be forwarded by the EDPB to the United States where the complaint will be investigated by the Civil Liberties Protection Officer.
- The second layer allows for the decision of the Civil Liberties Protection Officer to be appealed to the independent Data Protection Review Court, which is established under the Regulation on the Data Protection Review Court issued by the US attorney general and is entitled to request information from the intelligence agency in question and to take binding remedial measures, including deletion of the data.

This framework directly addresses the issues mentioned by the CJEU in the Schrems II Decision and was a key component that led to the adequacy decision. It is important to note, however, that these mechanisms have not yet been tested in practice, and we expect the initial application of the mechanisms to be heavily scrutinized by Max Schrems and other privacy activists.

WHAT COMES NEXT?

The EU adequacy decision takes formal effect 10 July 2023. However, the DPF only provides for a secure tool to legitimize transfers of personal data to US data importers where these importers have been certified under the DPF program. Certification includes provision of evidence that the minimum data protection standards are complied with by the importer. When the first US companies will be certified is still uncertain. It is also unclear whether the US companies that were or are already certified under the EU/US Privacy Shield framework will be able to leverage that compliance framework to certify under the DPF quickly or will have to run a new compliance effort from scratch.

Whether the new security restrictions offered and rights granted by the United States are sufficient to ensure an adequate level of protection of personal data against access by authorities and provides for sufficient redress rights for EU citizens (in particular whether an executive order is the correct legal mechanism as opposed to a formal legal act) remains to be seen. As was anticipated,NOYB has already announced its intent to have the CJEU review the DPF. Until the DPF has passed this ultimate judicial test (which may take up to several years), EU companies may be hesitant to rely solely on the DPF for sharing personal data with the United States. Best practice for now may still include a multi-level approach, involving the DPF (if the US company is certified under the DPF) and other tools, such as Standard Contractual Clauses.

Our Global Data Protection, Privacy, and Security team remains available to assist you in global and local cybersecurity matters from our offices in theAmericas, Europe, Middle East, Asia, and Australia.

KEY CONTACTS

WHITNEY E. MCCOLLUM
PARTNER

SEATTLE, SAN FRANCISCO
+1.206.370.7595
WHITNEY.MCCOLLUM@KLGATES.COM

DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM

