VAN BAEL & BELLIS

Client Alert | Data Protection

European Commission adopts Adequacy Decision for Transatlantic Transfers of Personal Data

On 10 July 2023, the European Commission (***EC***) adopted an adequacy decision for the EU-U.S. Data Privacy Framework (***DPF***). Under Chapter V of the General Data Protection Regulation (***GDPR***), transfers of personal data outside the European Union (***EU***) – and, by extension, the European Economic Area (***EEA***) – are prohibited unless the intended destination jurisdiction(s) offer(s) an "*adequate level of protection*" of personal data when compared to the one guaranteed in EU law (Article 45 GDPR), unless certain appropriate safeguards are put in place (Article 46 GDPR) or unless certain derogations apply (Article 49 GDPR). In turn, the United States (***US***) generally does not restrict data transfers to other jurisdictions.

Under EU law, an adequacy decision constitutes one of the key legal mechanisms for a transfer of personal data outside the EU/EEA. Such a decision, in essence, is a determination made by the EC that a given jurisdiction or a sector thereof, or an international organization, offers an adequate standard of protection of personal data. It hence allows for the unrestricted transfer of personal data from the EU/EEA to such a jurisdiction.

Previously, the US had installed two self-certification schemes that enjoyed adequacy status, but both have been annulled: the so-called Safe Harbor, from 2000 until its invalidation by the Court of Justice of the EU (***CJEU***) (judgment of 6 October 2015, *Schrems I*), and – subsequently – the Privacy Shield, from 2016 until its invalidation in 2020 (judgment of 16 July 2020, *Schrems II*).

More specifically, in *Schrems II,* the CJEU held that the limitations to the protection of personal data, resulting from US authorities' access to the said data for national security and law enforcement purposes, as well as the prescribed remedies, were not circumscribed in a such manner that met the necessary threshold of being "*essentially equivalent*" to those under EU law.

Therefore, the new arrangement, the DPF sets out to remedy these shortcomings, and to grant such a satisfactory level of protection to the individuals in the EU/EEA.

WHAT ARE THE NEW SAFEGUARDS INTRODUCED?

The adequacy decision – dated 10 July 2023 – entered into force on 11 July 2023, following a series of long, bilateral negotiations and the resulting changes in US surveillance law and practice. Most importantly, US President Biden's Executive Order 14086 of 7 October 2022 on "*Enhancing Safeguards for United States Signals Intelligence Activities*" and a Regulation on the Data Protection Review Court issued by the US Attorney General (14 October 2022) were meant to address previous EU/EEA data privacy concerns (raised especially in *Schrems II)* with the introduction of new binding safeguards.

One core element of the new safeguards introduced is that US authorities, in accessing the personal data of EU/EEA individuals, must

conduct a balancing test to ensure that any access to the said data is deemed necessary and proportionate. US authorities will also be subject to greater oversight – by both judicial and non-judicial bodies, such as the Privacy and Civil Liberties Oversight Board (***PCLOB***), the Department of Justice ***(DoJ)*** and various Committees in the US Congress – to ensure their compliance with these rules.

A further novelty is the establishment of an independent and impartial redress mechanism. Under the DPF, EU/EEA individuals can resolve their complaints before the so-called Data Protection Review Court ***(DPRC***). An EU/EEA individual wishing to lodge such a complaint must submit it to a relevant national Data Protection Authority (***DPA***) who will subsequently channel the complaint to the redress mechanism via the secretariat of the European Data Protection Board (***EDPB***).

HOW DOES DPF FUNCTION?

The DPF is a self-certification mechanism which is open to US organisations subjected to the jurisdiction of the Federal Trade Commission (***FTC***) or the Department of Transport (***DoT***). To benefit from the DPF, an American organisation receiving personal data from an EU/EEA exporter must certify their participation in the DPF by completing and sending a self-certification submission to the Department of Commerce (***DoC***). Organisations must also pay an annual fee to utilise the DFP, which is tiered based on their yearly income.

Once the DoC has determined that the initial self-certification is complete, the organization will be placed on the DPF List, which is public. From that moment, the organisation can rely on the Adequacy decision to transfer personal data from the EU/EEA to the US in compliance with Chapter V of the GDPR.

The DoC may remove an organisation from the list if the organisation voluntarily withdraws, fails to complete its annual re-certification, or if it persistently fails to comply with the DPF principles. Both the FTC and the DoT will monitor and enforce organisations' compliance with their obligations under the DPF itself.

WHAT ARE THE PRINCIPLES OF THE DPF?

The principles which organisations must comply with are listed in Annex I to the adequacy decision and can be summarised as follows:

1. **Notice** – informing individuals about, among others, participation in the DPF, the purposes of the data collection, and of any identities of third parties that may have access to the data;

2. **Choice** – allowing individuals to choose whether their personal data may be disclosed to a third party;

3. **Accountability for Onward Transfers** – additional responsibilities for an organisation intending to forward personal data;

4. **Security** – commitment to taking "*reasonable and appropriate*" security measures to protect personal data;

5. **Data Integrity and Purpose Limitation –** generally limiting processing of personal data to the purpose for which it was collected, or closely related to that purpose;

6. **Access** – allowing individuals to access their personal data, as well as providing them the ability to correct or delete mistakes;

7. **Recourse, Enforcement, and Liability** – a baseline standard for potential recourse, including a "*readily available independent recourse mechanism*" or "*follow-up procedures*" to verify an organisation's compliance, and an "*obligation to remedy*" any violation of these principles.

HOW DOES THE DPF APPLY TO TRANSFERS FROM THE UK?

Following the withdrawal of the United Kingdom (***UK***) from the EU (Brexit), the UK retained – until its own reform of data protection law takes place – the GDPR and all adequacy decisions until Brexit. However, the EU-US DPF – as concluded after 31 December 2020 – does not apply to the UK.

In turn, organizations in the UK wishing to transfer personal data to the US might benefit from the UK Extension to the DPF. Organisations must apply to the DoC separately to use this transfer mechanism. Organizations might self-certify as of 17 July 2023, yet they can start relying of this Extension – and, consequently, transfer personal data from the UK – once the UK Government recognizes the adequacy of protection provided thereby.

KEY TAKEAWAYS

Industry welcomed the new adequacy decision. In the short term, organisations can sign up to the principles, which are similar to the previous EU-US mechanism. They will need to ensure the necessary steps to maintain certification (e.g., informing data subjects of their rights under the DPF, aligning their privacy policies with the DPF and subsequently updating them regularly, and cooperating with DPAs where necessary). To facilitate this, both the EC and the EDPB have already published Q&As to offer clarification on certain points of the DPF.

On the longer term, the DPF, like its predecessors, is likely to be challenged before the CJEU which will then have to assess whether the updates to the mechanism suffice to confirm its validity. In parallel, the EC is obliged to periodically review all adequacy decisions (Article 45(3) GDPR) and the first review of this one will occur within one year, i.e., before 10 July 2024.

KEY CONTACTS

Thibaut D'Hulst
Counsel
tdhulst@vbb.com
+32 (0)2 647 73 50

Dariusz Kloza
dkloza@vbb.com
+32 (0)2 647 73 50

Orla Murnaghan
omurnaghan@vbb.com
+32 (0)2 647 73 50

Madison Graham