State of Play of the European Commission's Draft Adequacy Decision on the new EU-U.S. Data Privacy Framework

1. Introduction

On 13 December 2022, the European Commission published its draft adequacy decision on the future of international data transfers with the United States. The draft adequacy decision marked the launch of a process to adopt a new legal framework laying down rules for ensuring appropriate data protection for European citizens whose data is transferred across the Atlantic. More specifically, the Commission's draft decision was issued in the wake of the publication of the new EU-U.S. Data Privacy Framework (DPF), presented by European Commission President, Ursula von der Leyen, and U.S. President, Joe Biden, in March 2022, as well as the subsequent issuing of the U.S. Government's Executive Order to implement the EU-U.S. Data Privacy Framework. Both documents seek to address the concerns of the Court of Justice of the European Union's (CJEU) Schrems II decision from 2020, ruling in favour of abolishing the previous EU-U.S. data transfer framework (the so-called Privacy Shield) on the basis that the U.S. government did not ensure sufficient data protection measures for European citizens during transatlantic data transfers.

The Commission's draft adequacy decision constitutes an assessment of the transposition of the commitments of the U.S. Government, as laid down in its Executive Order, to adjust its national privacy legislation to EU standards in the same field, so as to allow frictionless data transfers to third countries based on a single framework legislative decision. The adequacy decision thus assesses whether there is "essential equivalence" between the EU data privacy legislation (e.g., under the General Data Protection Regulation (GDPR)) and the U.S. counterpart on this matter. Based on its review, the Commission has in its draft adequacy decision concluded "that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. DPF from a controller or processor in the Union to certified organisations in the United States" (Recital 7), meaning that "personal data transfers from controllers and processors in the Union to certified organisations in the United States may take place without the need to obtain any further authorisation" (Recital 8).

2. Scope and definitions of the EU-U.S. Data Privacy Framework

According to Recital 9 of the Commission's draft adequacy decision, the new EU-U.S. Data Privacy Framework (DPF) is based on a system of certification by which U.S. organisations commit to a set of privacy principles (the Principles). In order to be eligible for certification under the DPF, "organisations must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT)" (Recital 9). Organisations obtaining the certification will moreover be required to re-certify their adherence to the DPF Principles on an annual basis (see more under Point 2.3.1 on (Re-)certification). In terms of the definition of personal data, the DPF Principles align the definition with that of Regulation (EU) 2016/679 (GDPR). As such, personal data shall be understood as "data about an identified or identifiable individual that are within the scope of the GDPR received by an organisation in the U.S. from the EU, and recorded in any form" (Recital 11). Moreover, it also covers pseudonymised (or "key-coded") research data (including where the key is not shared with the receiving U.S. organisation).

Likewise, the notion of processing (of data) is defined as "any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination and erasure or destruction" (Recital 11).

Finally, referring to Recital 12, the DPF applies to organisations in the U.S. qualifying as *controllers* (meaning a person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data) or *processors* (i.e. agents acting on behalf of a controller). Accordingly, U.S. processors shall be contractually bound to act only on instructions from the EU controller and assists the controller in responding to individuals exercising their rights under the DPF Principles. "In the case of sub-processing, a processor must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Principles and take steps to ensure its proper implementation" (Recital 12).

3. Data Privacy Framework Principles

As briefly mentioned above, the new EU-U.S. Data Privacy Framework is built upon different Principles, which are formulated under the following overarching headlines: ***Notice***; ***Choice***; ***Accountability for Onward Transfer***; ***Security; Data Integrity and Purpose Limitation***; ***Access***; and ***Recourse, Enforcement, and Liability*** (Annex I, Section 2 of the European Commission's draft adequacy decision).

- **Purpose for processing data**

In accordance with the *Data Integrity and Purpose Limitation Principle*, following the logic of Article 5(1.b) of the GDPR, the DPF sets out that personal data shall be processed lawfully and fairly, collected for a specific purpose, and used only if such use is compatible with the purpose of the processing (Recital 13). This means that "an organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject" (Recital 14). If a controller or processors want to be able to use personal data for a new or different purpose, which is materially different yet still compatible with the original one, or disclose the data to a third party, the organisation in question must provide the data subject with the possibility of opting out pursuant to the *Choice Principle* (Recital 15).

- **Data accuracy, minimisation and security**

Recital 21 further addresses the *Data Integrity and Purpose Limitation Principle*, as it states that "personal data must be limited to what is relevant for the purpose of the processing. In addition, organisations must, to the extent necessary for the purposes of the processing, take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current." Furthermore, personal data must only be retained for as long as it serves the purpose(s) for which it was initially collected or subsequently authorised by the individual cf. the *Choice Principle* (Recital 22). The DPF Principles also address security, as they state that personal data should be processed in a manner ensuring data security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. As such, controllers and processors must take appropriate technical or organisational measures to protect personal data from potential security risks (Recital 23). Under the appertaining *Security Principle*, organisations are required "to take reasonable and appropriate security measures, taking into account the risks involved in the processing and the nature of the data" (Recital 24), thus laying down obligations similar to those of Article 32 of the GDPR.

- **Transparency**

Pursuant to Recital 25, "data subjects should be informed of the main features of the processing of their personal data." The DPF addresses this through its *Notice Principle,* which, similarly to the transparency requirements under the GDPR, lays down obligations for organisations to inform data subjects about e.g., "(i) the participation of the organisation in the DPF, (ii) the type of data collected, (iii) the purpose of the processing, (iv) the type or identity of third parties to which personal data may be disclosed and the purposes for doing so, (v) their individual rights, (vi) how to contact the organisation and (vii) available redress avenues" (Recital 26).

- **Individual rights**

Regarding the individual rights of data subjects, the DPF also includes an *Access Principle*, providing data subjects with the right to obtain confirmation from an organisation, without justification, of whether the organisation is "processing personal data related to them; have the data communicated to them; and obtain information about the purpose of the processing, the categories of personal data being processed and the (categories of) recipients to whom the data is disclosed" (Recital 30). Organisations receiving such access requests must respond within a reasonable period of time, but may also introduce reasonable limits to the number of times within a given period that a particular individual can request data access, as well as they may charge a fee for such operation e.g., were requests are deemed excessive, particularly due to their repetitive character (Recital 30). Another aspect addressed in relation to individual rights is that of personal data being used for direct marketing purposes, to which Recital 32 gives data subjects the general right of opting out from having processed their data for such purposes at any time.

Finally, although the DPF principles do not specifically address the issue of decisions affecting individuals based solely on the automated processing of personal data, any decision based on automated processing, in relation to personal data that has been collected in the EU, will typically be taken by the controller in the Union, which has a direct relationship with the data subject in question, and as such will be directly subject to the GDPR (Recital 33). "This includes transfer scenarios where the processing is carried out by a foreign (for instance U.S.) business operator acting as an agent (processor) on behalf of the controller in the Union (or as a sub-processor acting on behalf of the Union processor having received the data from a Union controller that collected it) which on this basis then takes the decision" (Recital 33).

- **Restrictions on onward transfers**

The DPF's *Accountability for Onward Transfer Principle* lays down special rules for so-called 'onward transfers', meaning transfers of personal data from an organisation certified under the EU-U.S. DPF to a third party controller or processor, irrespectively of the latter being located in the U.S. or a third country outside the EU or U.S. (Recital 38). Accordingly, any onward transfer can only take place either for limited and specified purposes; on the basis of a contract between the DPF organisation and the third party; and only if that contract requires the third party to provide the same level of protection as the one guaranteed by the DPF Principles (Recital 38).

- **Accountability**

The DPF Principles also set out rules ensuring that organisations participating in the DPF are held accountable for their compliance with said Principles. As such, Recital 45 stresses that once an organisation has voluntarily decided to certify under the EU-U.S. DPF, it must effectively comply with the Principles, which will be compulsory and enforceable upon the organisation. This is further elaborated in the same

recital, stating that "this can be done through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies" (Recital 45). Finally, "organisations must retain records on the implementation of their EU-U.S. DPF practices and make them available upon request in the context of an investigation or a complaint" (Recital 46).

- **Compliance monitoring and enforcement**

Recital 54 addresses monitoring of compliance with the DPF Principles. More specifically, it states that in cases where there is credible evidence that an organisation is non-compliant with its commitments under the DPF (including if the U.S. Department of Commerce (DoC) receives complaints or the organisation does not respond satisfactorily to inquiries of the Doc), the DoC will require the organisation to complete and submit a detailed questionnaire. If the given organisation fails to satisfactorily and timely reply to the questionnaire, it will subsequently be referred to the relevant authority (the FTC or DoT) for possible enforcement action (Recital 54).

Regarding enforcement of the Principles, Recital 58 further elaborates that "in order to ensue that an adequate level of data protection is guaranteed in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place". As such, DPF certified organisations must be subject to the jurisdiction of the competent U.S. authorities, that is the FTC and DoT, which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles (Recital 59).

- **Redress mechanisms**

The DPF's *Recourse, Enforcement and Liability Principle* requires organisations to provide recourse for individuals affected by an organisation's non-compliance, and thus the possibility for EU data subjects to lodge complaints regarding non-compliance and to have these complaints resolved, if necessary, by a decision that provides effective remedy (Recital 65). DPF organisations are, however, free to choose independent recourse mechanisms in either the EU or the U.S. (Recital 66). In terms of the concrete redress avenues a data subject can make use of, the DPF sets out different options:

1) EU data subjects may pursue cases of non-compliance with the Principles through the direct contacts with the EU-U.S. DPF organisations. To facilitate resolutions, the organisations must put in place an effective redress mechanism to deal with such complaints (Recital 68).

2) Individuals can also bring a complaint directly to the independent dispute resolution body (in the EU or the U.S.) designated by an organisation to investigate and resolve individual complaints (Recital 69).

3) Individuals may also bring their complaints to a national Data Protection Authority (DPA) in the EU (Recital 72).

4) Moreover, the DoC has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the DPF Principles. To this end, the DoC provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with organisations to facilitate resolution (Recital 77).

5) A DPF organisation must be subject to the jurisdiction of U.S. authorities, and in particular the FTC, which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles (Recital 79).

6) In case none of the other available redress mechanisms have resolved an individual's complaint, the EU data subject may proceed to the recourse mechanism of last resort, which allows the individual to invoke binding arbitration by the DPF panel (for more information on the DPF panel, see Recital 81-84 of the draft adequacy decision). In relation to this, organisation must inform the data subjects about their possibility to invoke binding arbitration and they are obliged to respond once an individual has invoked this option by delivering notice to the concerned organisation (Recital 80).

7) Finally, where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress are available under U.S. law, including the possibility to obtain compensation for damages (Recital 85).

4. Access and use of personal data transferred from the EU by public authorities in the U.S.

The European Commission's draft adequacy decision also addresses the potential access and use of EU citizens' personal data by U.S. public authorities following transatlantic data transfers (Point 3 of the draft adequacy decision). More specifically, the Commission has assessed "the limitations and safeguards, including the oversight and individual redress mechanisms available in United States law as regards the collection and subsequent use by U.S. public authorities of personal data transferred to controllers and processors in the U.S. in the public interest, in particular for criminal law enforcement and national security purposes" (Recital 86). Based on its findings, the Commission has then in its draft decision concluded that the conditions under which government access to data transferred to the U.S. serve as 'essentially equivalent' pursuant to Article 45(1) of the GDPR (Recital 86). The Commission has conducted its assessment based on a number of criteria, taking into account in particular that "any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation to the exercise of the right concerned" (Recital 87). Moreover, Recital 87 further elaborates that "in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the Union, this legal basis must lay down clear and precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse" (Recital 87). Finally, "these rules and safeguards must be legally binding and enforceable by individuals. In particular, data subjects must have the possibility of bringing legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data" (Recital 87). A detailed explanation of the specific redress mechanisms that allow individuals to obtain access to their personal data, to establish the lawfulness of government access to their data, and, in case a violation is found, to have such violation remedied, can be found under *Point 3.2.3 Redress* of the draft adequacy decision.

5. Assessment by the European Data Protection Board

In the wake of the publication of the European Commission's draft adequacy decision, the following step in the procedure of formally adopting the new EU-U.S. Data Privacy Framework has been for the European Data Protection Board (EDPB) to issue its expert opinion as to whether it also finds the U.S.' new data protection measures to be 'essentially equivalent' to those of the EU. On 28 February, the EDPB then published its opinion, which suggest the Commission to improve certain parts of the text. Although the EDPB acknowledge that the new EU-U.S. DPF contains "substantial improvements" to the previous agreement on the matter, the Board is still concerned about several parts of the agreement, and in particular points out a lack of safeguards for the U.S. intelligence services' access to Europeans' data. Moreover, the EDPB also highlights lack of progress in relation to the rights of citizens, as these are considered to be "essentially the same" as in the previous Privacy Shield agreement. With that being said, the EDPB welcomes the introduction of legal concepts, such as 'necessity' and 'proportionality' for U.S. intelligence services' access to EU citizens' data, as well as it applauds the set up of a new redress mechanism. The EDPB expert opinion is non-binding of nature, however, the Board's rather lukewarm evaluation of the draft adequacy decision might lead the Commission to go back to the drawing board to modify those parts of the text that might challenge the DPF in case of a judicial review by the CJEU.

6. Draft motion for a resolution by European Parliament's LIBE Committee

On 1 March, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), in charge of the Parliament's position on the EU-U.S. Data Privacy Framework, held its first debate on its Draft Motion for a Resolution on the Commission's draft adequacy decision. The LIBE Draft Motion, similarly to the EDPB's opinion, acknowledge the efforts made in the U.S. Executive Order regarding the introduction of the legal principles of proportionality, necessity, and the legitimate objectives for these. With that being said, the Draft Motion generally concludes that the new DPF fails to provide equivalent data protection for European citizens, whose data is transferred from the EU to the U.S. For instance, the draft text stresses that the legal principles mentioned above are long-standing principles in the EU data protection regime, and that the definitions of these principles in the U.S. Executive Order do not align with their EU counterparts and their interpretation by the CJEU. Furthermore, the Draft Motion is also critical towards the so-called Data Protection Review Court (DPRC), established by the U.S. via its Executive Order, as its decisions will be classified; as the DPRC will be part of the executive branch and not the judiciary; and as the redress mechanism does not set up an obligation to notify the complainant that their personal data has been processed. As such, the Draft Motion argues that the DPRC undermines the right to access or to rectify personal data. The text further points to the unpredictable applicability of the Executive Order, as the U.S. President is empowered to, at any time, expand the list of legitimate national security objectives, which provides as a condition for derogating from the rules laid down in the Executive Order. Moreover, the Draft Motion also acknowledges that European businesses need and deserve legal certainty, and that the repeal of the previous data transfer agreement has created additional costs for businesses, including small and medium-sized enterprises. Finally, the text also addresses commercial matters, stating that "remedies for commercial matters under the adequacy decision are insufficient, and that remedies are largely left to the discretion of companies."

On a more general note, the LIBE Draft Motion also argues that current U.S. domestic law is incompatible with the GDPR, for instance because the U.S. still do not have a federal data protection law, unlike all other third countries that have received an adequacy decision under the GDPR, for which reason the Committee

advices against entering into a new data transfer agreement, until the domestic data legislation of the U.S. is more aligned to that of the EU.

7. Next steps

The next steps in the procedure to adopt a new EU-U.S. Data Privacy Framework is for the EU member states to vote on the adequacy decision by means of the comitology procedure. Moreover, the European Parliament's LIBE Committee, and eventually the Parliament as a whole, will have to finalise its position on the matter. The Parliament's final Motion for Resolution is expected to be adopted by mid-April. In addition, national DPAs will also be able to provide their input to the adequacy decision. Depending on the views and positions of the various actors involved in the legislative process, the Commission might have to review its draft decision. However, European Commissioner for Justice, Didier Reynders, has previously expressed that he expects the new data transfer framework to be formally adopted by summer.