Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework

Adopted on 28 February 2023

Executive summary

On 13 December 2022, the European Commission published a draft adequacy decision ('Draft Decision') which includes annexes constituting a new framework for transatlantic exchanges of personal data, the EU-U.S. Data Privacy Framework ('DPF'), which is meant to replace the previous U.S. Privacy Shield invalidated by the Court of Justice of the European Union ('CJEU') on 16 July 2020, in the Schrems II case. The key component of the DPF is the EU-US Data Privacy Framework Principles, including the Supplemental Principles (collectively 'the DPF Principles').

In accordance with Article 70(1)(s) of Regulation (EU) 2016/679[1] of the European Parliament and of the Council ('GDPR'), the Commission requested the opinion of the European Data Protection Board ('EDPB') on the Draft Decision.

The EDPB assessed the adequacy of the level of protection afforded in the USA, on the basis of the examination of the Draft Decision. The EDPB assessed both the commercial aspects and the access to and use of personal data transferred from the EU by public authorities in the US.

The EDPB took into account the applicable EU data protection legal framework as set out in the GDPR, as well as the fundamental rights to private life and data protection as enshrined in Articles 7 and 8 of the Charter of Fundamental rights of the European Union and Article 8 of the European Convention on Human Rights. It also considered the right to an effective remedy and to a fair trial laid down in Article 47 of the Charter, as well as the jurisprudence related to the various fundamental rights.

In addition, the EDPB has considered the requirements of the Adequacy Referential adopted by the EDPB[2].

The EDPB's key objective is to give an opinion to the Commission on the adequacy of the level of protection afforded to individuals whose personal data is transferred to the US. It is important to recognise that the EDPB does not expect the US data protection framework to replicate European data protection law.

However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the CJEU require the third country's legislation to provide data subjects with a level of protection essentially equivalent to that guaranteed in the EU.

1.1. General data protection aspects

The DPF provides that adherence to the DPF Principles by DPF Organisations may be limited in some cases (e.g. to the extent necessary to comply with a court order or to meet public interest). In order to better identify the impact of these exemptions on the level of protection for data subjects, the EDPB recommends that the Commission includes in the Draft Decision clarification on the scope of the exemptions, including on the applicable safeguards under US law.

The EDPB notes that the structure of the annexes and their numbering makes the information rather difficult to find and refer to. This contributes to an overall complex presentation of the new framework,

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

[2] Art. 29 Working Party, Adequacy Referential, WP 254 rev.01, 28 November 2017, as last revised and adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018 (hereinafter 'Adequacy Referential').

which compiles in its annexes documents of different legal value, and may not favour a good understanding of the DPF Principles by data subjects, DPF Organisations, and EU Data Protection Authorities. The EDPB also stresses that the terminology should be used consistently throughout the DPF. Similarly, the definition of some essential terms is lacking[3].

The EDPB welcomes the updates made to the DPF Principles[4], which will constitute the binding legal framework for DPF Organisations, but notes that despite a number of changes and additional explanations made in the recitals of the Draft Decision, the DPF Principles to which the DPF organisations have to adhere remain essentially unchanged with regard to those applicable under the Privacy Shield (on which were based the Working Party 29 ('WP29') and EDPB annual joint reviews). The DPF Principles are also, to a large extent, the same as those of the draft Privacy Shield on which the WP29 based its 2016 opinion[5]. For those DPF Principles that are substantially unchanged, the EDPB considers not necessary to repeat all comments previously made by the WP29. The EDPB has decided to focus on specific aspects that it considers to be even more relevant today, in view of the evolution of the legal and technological environment.

For instance, the EDPB notes that some issues of concern previously raised by the WP29 and the EDPB in relation to the Privacy Shield principles remain valid. In particular, these relate to the rights of data subjects (e.g. some exceptions to the right of access and the timing and modalities for the right to object), the absence of key definitions, the lack of clarity in relation to the application of the DPF Principles to processors, and the broad exemption for publicly available information[6].

The EDPB would also like to reiterate that the level of protection of individuals whose data is transferred must not be undermined by onward transfers from the initial recipient of the transferred data[7]. The EDPB invites once more the Commission to clarify that the safeguards imposed by the initial recipient on the importer in the third country must be effective in light of third country legislation, prior to an onward transfer in the context of the DPF.

Rapid developments in the field of automated decision-making and profiling - increasingly by means of AI technologies- call for particular attention. The EDPB welcomes the Commission's references to specific safeguards provided by relevant US law in different fields[8]. However, the level of protection for individuals seems to vary according to which sector-specific rules - if any- apply to the situation at hand. The EDPB maintains that specific rules concerning automated decision-making are needed in order to provide sufficient safeguards, including the right for the individual to know the logic involved, to challenge the decision and to obtain human intervention when the decision significantly affects him or her.

The EDPB recalls the importance of effective oversight and enforcement of the DPF and considers that compliance checks as regards more substantive requirements are crucial. These aspects will be closely monitored by the EDPB, including in the context of the periodic reviews. The EDPB takes note of the renewed commitments in the letters from the Federal Trade Commission ('FTC')[9] and the Department

[3] This is the case for the terms 'agent' and 'processor'. Moreover, the concept of 'human resources (HR) data' still needs to be discussed with US authorities.
[4] For instance, the clarification that key-coded data are personal data.
[5] Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016 (hereinafter, 'WP29 Opinion 01/2016').
[6] EU.U.S. Privacy Shield - Third Annual Joint Review, EDPB report adopted on 12 November 2019, para. 11.
[7] GDPR Adequacy Referential, 3.A.9.
[8] Draft Decision, Recital 35.
[9] Draft Decision, Annex IV.

of Transportation ('DOT')[10] as regards enforcement e.g. to prioritise the investigation of alleged DPF violations.

The EDPB notes that seven redress avenues are provided to EU data subjects, if their personal data are processed in violation of the DPF. These redress mechanisms are the same as those included in the former Privacy Shield, which had been subject to comments by the WP29[11]. The effectiveness of these redress mechanisms will be closely monitored by the EDPB, including in the context of the periodic reviews.

1.2. Access and use of personal data transferred from the European Union by public authorities in the US

In the Draft Decision, the European Commission concludes that "any interference in the public interest, in particular for criminal law enforcement and for national security purposes, by U.S. public authorities with the fundamental rights of the individuals whose personal data are transferred from the Union to the United States under the EU-U.S. Data Privacy Framework, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists"[12].

The European Commission reaches its conclusion after an extensive assessment of the Executive Order 14086 enhancing safeguards for U.S. signals intelligence activities (EO 14086). The EO 14086 was issued by the U.S. President on 7 October 2022, following negotiations of the European Commission with the U.S. Government in the wake of the invalidation of the previous adequacy decision, called the Privacy Shield, by the Court of Justice of the European Union (CJEU).

The EDPB would welcome that not only the entry into force but also the adoption of the decision are conditional upon inter alia the adoption of updated policies and procedures to implement EO 14086 by all US intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share this assessment with the EDPB.

With regard to governmental access to personal data transferred to the U.S., the EDPB has focussed its analysis on the assessment of the new EO 14086, as it is effectively meant to address and remedy the deficits identified by the CJEU in its Schrems II ruling when it found the previous adequacy decision to be invalid.

The EDPB recognises that the U.S. legal framework for signals intelligence activities has been amended by adoption of EO 14086 and regards the additional safeguards included in this order as a significant improvement. The EO 14086 introduces the concepts of necessity and proportionality into the U.S. legal framework on signals intelligence, and it provides, if the EU were to be designated as a qualifying regional economic integration organisation, a new redress mechanism for EU individuals. The EDPB considers the new redress mechanism to be significantly improved compared to the previous so-called Ombudsperson mechanism under the Privacy Shield. In contrast to the previous legal framework, which did not create rights for EU individuals, as was explicitly noted by the CJEU, the new EO 14086 creates such entitlements, and it provides more safeguards for the independence of the Data Protection Review Court, and more effective powers to remedy violations.

When comparing the additional safeguards included in EO 14086 to what the EDPB has framed the European Essential Guarantees (EEGs), as the standard elaborated on the basis of the jurisprudence of

[10] Draft Decision, Annex V.
[11] See in particular WP29 Opinion 01/2016, Section 2.2.6 (a).
[12] Draft Decision, Recital 195.

the CJEU and the European Court of Human Rights (ECtHR), the EDPB has still identified in its assessment a number of points for additional clarifications, for attention or for concern. These points reflect that, while the EDPB based its opinion on the Schrems II ruling, the scope of the EDPB's assessment necessarily includes considerations that go beyond the specific findings in the Schrems II judgment.

The EDPB sees a need for further clarification on questions, in particular, relating to "temporary bulk collection", and to the further retention and dissemination of the data collected (in bulk) in the U.S. legal framework.

As the test of essential equivalence is not a test of identity, and as the safeguards included in the new legal framework on signals intelligence have been strengthened, the EDPB's main point of attention and of concern is focused on an assessment of the safeguards in their entirety, following a holistic approach covering the safeguards for the entire cycle of processing, from the collection of data to the dissemination of data, and including the elements of oversight and redress.

In this regard, the EDPB emphasises the following findings:

While the EDPB recognises that the EO 14086 introduces the concepts of necessity and proportionality in the legal framework of signals intelligence, it underlines the need to closely monitor the effects of these amendments in practice, including the review of internal policies and procedures implementing the EO's safeguards at agency level.

The EDPB also welcomes the fact that the EO 14086 contains a list of specific purposes for which collection can and cannot take place, while noting the objectives may be updated with additional – not necessarily public – objectives in the light of new national security imperatives.

As a deficit in the current framework, the EDPB has in particular identified that the U.S. legal framework, when allowing for the collection of bulk data under Executive Order 12333, lacks the requirement of prior authorisation by an independent authority, as required in the most recent jurisprudence of the ECtHR, nor does it provide for a systematic independent review ex post by a court or an equivalently independent body. With regard to prior independent authorisation of surveillance under Section 702 FISA, the EDPB regrets that the FISA Court ('FISC') does not review a programme application for compliance with the EO 14086 when certifying the programme authorising the targeting of non-U.S. persons, even though the intelligence authorities carrying out the programme are bound by it. In the view of the EDPB, the additional safeguards contained in this order should nevertheless be taken into account including by the FISC. The EDPB recalls that reports of the Privacy and Civil Liberties Oversight Board ('PCLOB') would be particularly useful to assess how the safeguards of the EO 14086 will be implemented and how these safeguards are applied when data is collected under Section 702 FISA and EO 12333.

On the redress mechanism, the EDPB recognises significant improvements relating to the powers of the Data Protection Review Court ('DPRC') and its enhanced independence compared to the Ombudsperson. The EDPB also recognises the additional safeguards foreseen in the new redress mechanism such as the role of the special advocates that includes advocating regarding the complainant's interest as well as the review of the redress mechanism by PCLOB. While taking into account the nature of national security and the safeguards provided in EO 14086, the EDPB is nevertheless concerned about the general application of the standard response of the DPRC notifying the complainant that either no covered violations were identified or a determination requiring appropriate remediation was issued, and its non-appealability, taken together. Given the importance

of the redress mechanism, the EDPB calls on the Commission to closely monitor the practical functioning of this mechanism.

The EDPB expects the Commission to follow up on their commitment to suspend, repeal or amend the adequacy decision on grounds of urgency, in particular if the U.S. Executive would decide to restrict the safeguards included in the EO[13].

Overall, the EDPB positively notes the substantial improvements the EO offers compared to the previous legal framework, in particular as regards the introduction of the principles of necessity and proportionality and the individual redress mechanism for EU data subjects. Given the concerns expressed and the clarifications required, the EDPB suggests these concerns should be addressed and that the Commission provides the requested clarifications in order to solidify the grounds for the Draft Decision and to ensure a close monitoring of the concrete implementation of this new legal framework, in particular the safeguards it provides, in the future joint reviews.

[13] Draft Decision, Recital 212.

Table of contents

The European Data Protection Board

The European Data Protection Board has adopted the following statement:

Having regard to Article 70(1)(s) of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter 'GDPR')[1],

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[2],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION

1 INTRODUCTION

1.1 US data protection framework

1. The United States ('US') and the European Union ('EU') have different approaches to privacy and data protection. While privacy and data protection in the EU are fundamental rights guaranteed in Articles 7 and 8 of the European Charter of Fundamental Rights, data protection in the US is generally approached from a consumer protection perspective. As a result, regulatory approaches in the US and EU differ[3].

2. Differing from the EU comprehensive approach taken by the GDPR, in the US, no comprehensive general law on data protection exists at federal level. The protection of privacy in the US is rather realised by a sectoral and state approach. For instance, some specific sectors are covered by specific acts, e.g.:

   - Health Insurance Portability and Accountability Act (HIPAA)[4]

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1.

[2] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

[3] See also European Commission Draft Implementing Decision 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, published on 13 December 2022 (hereinafter, the 'Draft Decision'), Annex I, Section I.

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law. It creates national standards to protect patients' sensitive health information. The goal of HIPAA is to adequately protect individuals' health information, while allowing health information to flow for the delivery and promotion of high quality health care. HIPAA governs the use and disclosure of health information by entities subject to the Privacy Rule. It also includes standards for the rights of individuals to understand and control how their health information is used.

- Children's Online Privacy Protection Act (COPPA)[5]
- Gramm-Leach-Billey Act (GLBA)[6]

3. In the field of government access to personal data transferred from the EU to the US a number of different legal bases, limitations and safeguards apply. The legal processes for access to information for law enforcement purposes stem either from the U.S. Constitution directly (the Fourth Amendment), from statutory and procedural law or from Guidelines and Policies of the Department of Justice at federal level or at state level. Access to information for national security purpose is governed by several legal instruments and in particular by the Foreign Intelligence Surveillance Act (FISA), the Executive Order 12333, the recently adopted Executive order 14086 as well as the Attorney General regulation ('AG Regulation')[7] establishing a Data Protection Review Court ('DPRC').

4. On 13 December 2022, the Commission issued its draft Commission Implementing Decision 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 ('the Draft Decision'), which contains in its annex the EU-US Data Privacy Framework ('the DPF'). For the reasons explained above, the Draft Decision is not based on a specific and comprehensive federal legal framework, but on the DPF.

5. The DPF works as follows: *'The U.S. Department of Commerce ("the Department") is issuing the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively "the Principles") and Annex I of the Principles ("Annex I"), under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512)'*[8].

6. The development of the 'Principles' ('the DPF Principles') was conducted under consultation of the European Commission ('the Commission'), industry and other stakeholders in order to achieve the goal of the facilitation of EU–U.S. trade and commerce[9], while ensuring that data subjects are provided with a level of protection that is essentially equivalent to that guaranteed in the EU.

7. The DPF Principles are described as a 'key component' of the DPF. On the one hand, they provide a 'ready-to-use mechanism' for data transfers from the EU to the US. On the other hand, personal data transferred from the EU to the US is safeguarded and protected as required by EU law.

---

https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] The primary goal of COPPA is to place parents in control over what personal information is collected form their children under 13 from operators of child-directed websites and online services (including mobile apps and IoT devices, such as smart toys) or general audience sites. COPPA requires that these operators parental notice and has to obtain verifiable parental consent. This also applies to data from foreign children if the websites or services are operated in the U.S. and subject to COPPA. At the same time, the regulations also apply to foreign-based websites and services if they are directed at children in the US. See: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions and Draft Decision, Annex IV, p. 3.

[6] One of the goals of the Gramm-Leach-Bliley Act is to protect consumer privacy in the financial sector. The GLB Act requires financial institutions to explain to their customers their information-sharing practices and to create safeguards to protect customer information (e.g., for companies regulated by the FTC under the FTC Safeguards Rule). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] Attorney General Order No. 5517-2022, which amends US Department of Justice regulations as authorised and directed by EO 14086.

[8] Draft Decision, Annex I, Section I.

[9] *Ibid*.

8. The DPF is only applicable for US organisations who have self–certified themselves according to the requirements of the framework ('DPF Organisations'). For the time being, this is only possible if they fall under the jurisdiction of the Federal Trade Commission ('FTC') or the Department of Transportation ('DoT'). In the future, other statutory bodies – with competence to supervise the implementation of the DPF Principles - might be added in a future annex.

9. It is explained by the DPF Principles that the conditions of the framework are enforceable by (i) the FTC under Section 5 of the Federal Trade Commission Act (FTC Act) prohibiting unfair or deceptive acts in or affecting commerce[10], (ii) the DoT under 49 U.S.C: § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation for the sale or of air transportation or (iii) under other laws or regulations by which such acts are prohibited.

10. It is pointed out in the DPF Principles that neither the GDPR is affected in its application nor existing privacy obligations, otherwise applied under US law, are limited by the DPF Principles.

1.2 Scope of the EDPB's assessment

11. The Draft Decision reflects the Commission's assessment of the DPF, which is the outcome of discussions with the US government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an opinion on the Commission's findings as regards the adequacy of the level of protection in a third country and, if needed, endeavour to make proposals to address any issue.

12. The EDPB welcomes the updates made to the DPF Principles[11], which will constitute the binding legal framework for DPF Organisations. However, the EDPB notes that the DPF Principles remain essentially the same as those under the Privacy Shield[12] (on which were based the Working Party 29 ('WP29') and EDPB annual joint reviews). The DPF Principles are also, to a large extent, the same as those of the draft Privacy Shield on which the WP29 based its 2016 opinion[13] ('the WP29 Opinion 01/2016'). For those DPF Principles that are substantially unchanged, the EDPB considers not necessary to repeat all comments previously made by the WP29. The EDPB has decided to focus on specific aspects that it considers to be even more relevant today, in view of the evolution of the legal and technological environment.

13. In addition, in line with the jurisprudence of the CJEU[14], a very important part of the analysis covers the legal regime of government access to personal data transferred to the US.

14. In its assessment, the EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the EU Charter of Fundamental Rights ('the Charter'), respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial, and Article 8 of the European Convention on Human Rights ('ECHR') protecting the right to private and family life. In addition to the above, the EDPB considered the

[10] 15 U.S.C. § 45 (a).
[11] For instance, the clarification that key-coded data are personal data.
[12] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p. 1.
[13] Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016 (hereinafter, 'WP29 Opinion 01/2016').
[14] In particular: Judgment of the Court of Justice of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner,* C-392/14, ECLI:EU:C:2015:650, and Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* C-311/18, ECLI:EU:C:2020:559.

requirements of the GDPR, the relevant case law and the Adequacy Referential adopted by the EDPB ('the GDPR Adequacy Referential')[15].

15. The objective of this exercise is to provide the Commission with an opinion on the assessment of the adequacy of the level of protection provided by the DPF. The concept of 'adequate level of protection', which already existed under Directive 95/46, has been further developed by the CJEU. It is therefore important to recall the standard set by the CJEU in its Schrems I[16] (invalidating the 'Safe Harbor')and Schrems II[17] (invalidating the Privacy Shield) judgments.

16. In its Schrems I judgment, the CJEU ruled that, while the 'level of protection' in the third country must be 'essentially equivalent' to that guaranteed in the EU – *'the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU'*[18]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process personal data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[19].

17. In its Schrems II decision, the CJEU found that the laws on the basis of which U.S. intelligence authorities can access personal data transferred to the U.S. (Section 702 FISA/E.O. 12333) disproportionately restrict the rights enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (the Charter) and are thus not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter[20].

18. Moreover, the CJEU stated that the previous legal framework did not provide guarantees essentially equivalent to those required by Article 47 of the Charter as the Ombudsperson mechanism could not compensate, for the fact that neither PPD-28 nor E.O. 12333 grant non-U.S. persons an effective remedy[21]. The Ombudsperson lacked independence from the executive and the power to adopt binding decisions on U.S. intelligence services[22].

19. EO 14086, which generally replaces PPD-28, introduced two new requirements under US law which echo the CJEU Schrems II judgment: on the one hand, that signals intelligence activities shall be conducted only as far as necessary to advance a validated intelligence priority collection and only to

[15] Art. 29 Working Party, Adequacy Referential, WP 254 rev.01, 28 November 2017, as last revised and adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018 (hereinafter 'GDPR Adequacy Referential').
[16] CJEU Schrems I Judgment of the Court of Justice of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner,* C-392/14, ECLI:EU:C:2015:650 (hereinafter, 'CJEU Schrems I Judgment').
[17] Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* C-311/18, ECLI:EU:C:2020:559 (hereinafter, 'CJEU Schrems II Judgment').
[18]CJEU Schrems I Judgment, paras. 73-74.
[19] GDPR Adequacy Referential, p.2.
[20] CJEU Schrems II Judgment, paras. 184-185.
[21] CJEU Schrems II Judgment, para. 192.
[22] CJEU Schrems II Judgment, para. 195.

the extent and in a manner that is proportionate to the validated intelligence priority; and on the other hand, a redress mechanism.

20. In this opinion, the EDPB particularly assesses to which extent the DPF as well as the recently adopted EO 14086 effectively address the findings made by the CJEU in its judgment.

1.3 General comments and concerns

1.3.1 Assessment of the domestic law

21. The EDPB understands that the assessment contained in the Draft Decision relates to the DPF Principles. Nevertheless the EDPB would welcome some information about the US legal context, in which the DPF Organisations are operating. This would allow a better understanding of the interaction of the DPF with US law. For example, in Annex I 1[23] it is determined that the DPF Principles do not '*[…] limit privacy obligations that otherwise apply under U.S. law*', without describing these obligations.

1.3.2 International commitments entered into by the U.S.

22. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential, when assessing the adequacy of the level of protection of a third country, the Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations.

23. The US is a party to several international agreements that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16). Furthermore, the US, as an OECD member, adheres to the OECD Privacy Framework, in particular the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. On 14 December 2022, the OECD 'Declaration on Government Access to Personal Data held by Private Sector Entities' was adopted by Ministers and high-level representatives of OECD Members and the European Union. The US is also a party to the Budapest Convention on Cybercrime.

24. In addition, the US is a member of the Asia-Pacific Economic Cooperation ('APEC') Cross-Border Privacy Rules (CBPR) system, which is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized privacy rules. These privacy rules have been endorsed by APEC Leaders.

25. The EDPB also takes note of the participation of the US as Observer State in the work of the Consultative Committee of the Council of Europe Convention 108.

26. Furthermore, the EDPB takes note of and welcomes the continuous engagement of US bodies in the 2021 newly established format of the 'Roundtable of G7 Data Protection and Privacy Authorities' (G7 DPA Roundtable), which convenes independent data protection and privacy supervisory authorities of G7 countries. In this context, they have supported, for example, the latest G7 DPA Roundtable

[23] Draft Decision, Annex I, Section I, last sentence.

communiqué[24] adopted on 8 September 2022 in Bonn, Germany, which focussed on the concept of 'Data Free Flow with Trust'.

1.3.3 Progress in the area of US data protection legislation

27. The EDPB takes particular note of developments in data privacy legislation at state level in the US. The EDPB welcomes the adoption of data protection laws that have entered into force or will enter into force by 2023 in five States (California, Colorado, Connecticut, Virginia and Utah)[25].

28. The EDPB also notes that corresponding initiatives for further State laws have already been launched in many other US States.

29. Furthermore, the EDPB explicitly welcomes the efforts regarding the bipartisan initiative for a federal data protection law, the American Data Privacy and Protection Act (ADPPA).

1.3.4 Scope of the Draft Decision

30. According to Article 1 of the Draft Decision, the Commission concludes that the US ensures an adequate level of protection for personal data transferred from the EU to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce ('DoC'), in accordance with Section I.3 of Annex I[26].

31. The DPF is available to companies under the jurisdiction of the FTC or the DoT. It is pointed out that other US statutory bodies with similar powers might be added in future[27].

1.3.5 Limitations to the duty to adhere to the DPF Principles

32. Annex I, I.5. provides that adherence to the DPF Principles by DPF Organisations may be limited, among others, (i) to the extent necessary to comply with a court order or to meet public interest, law enforcement[28], or national security requirements[29] (including where statute or government regulation create conflicting obligations) and (ii) by statute, court order, or government regulation that creates explicit authorisations, provided that, in exercising any such authorisation, a DPF organisation can demonstrate that its non-compliance with the DPF Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.

---

[24] Roundtable of G7 Data Protection and Privacy Authorities, Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces, 8 September 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] California Consumer Privacy Act (2018; effective Jan. 1, 2020); California Privacy Rights Act (2020; fully operative Jan. 1, 2023); Colorado Privacy Act (2021; effective July 1, 2023); Connecticut Data Privacy Act (2022; effective July 1, 2023); Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023); Utah Consumer Privacy Act (2022; effective Dec. 31, 2023).

[26] Draft Decision, Final Considerations, Article 1, p. 57. The EDPB understands that the Draft Decision will not cover transfers from entities located outside the EU but subject to the GDPR by virtue of Article 3(2) GDPR to certified entities in the US.

[27] Draft Decision, Annex I, Section I.2.

[28] See Section 3.1 of the present opinion for more comments on the use of personal data covered by the EU-U.S. DPF for law enforcement purposes.

[29] See Section 3.2 of the present opinion for more comments on the use of personal data covered by the EU-U.S. DPF for national security purposes.

33. Without full knowledge of US law at both the federal and state level, it is difficult for the EDPB to assess in detail the scope of the exemptions listed in this paragraph. Therefore, the EDPB recommends that the Commission includes in the Draft Decision clarification on the scope of the exemptions, including on the applicable safeguards under US law, in order to better identify the impact of these exemptions on the level of protection for data subjects. The EDPB also underlines that the Commission should be informed of and monitor the application and adoption of any statute or government regulation that would affect adherence to the DPF Principles.

1.3.6 Changes with regard to the 'Privacy Shield'

34. The EDPB welcomes the effort made to address the requirements of the Schrems II judgment. Nevertheless, the EDPB would have welcomed, if more issues identified (i) in the WP29 Opinion 01/2016 and (ii) in the past joint reviews[30], would have been also addressed on the occasion of the negotiations of the DPF.

35. The EDPB also notes that despite a number of changes and additional explanations made in the recitals of the Draft Decision, the DPF Principles to which the DPF Organisations have to adhere remain essentially unchanged with regard to those applicable under the Privacy Shield.

1.3.7 Lack of clarity in the documents of the DPF

36. The EDPB notes that the structure of the annexes and their numbering makes the information rather difficult to find and refer to. This contributes to an overall complex presentation of the new framework, which compiles in its annexes documents of different legal value, and may not favour a good understanding of the DPF Principles by data subjects, DPF Organisations, and EU Data Protection Authorities ('EU DPA's').

37. The EDPB also stresses that the terminology should be used consistently throughout the DPF. This is currently not the case, for example, for the notion of 'processing'. Indeed, some of the parts of the DPF enumerate some types of data processing operations instead of making use of the term 'processing'. This may result in legal uncertainty and possible loopholes in the protection[31]

38. The EDPB welcomes that definitions of some of the terms used are included in the DPF[32]. However, this is not the case for some other essential terms such as at least 'agent' or 'processor', which in the view of the EDPB warrant a clear and specific definition in Annex I, I 8 of the DPF, and on which both the US and the EU agree, in order to avoid confusion at a later stage for DPF Organisations relying on the DPF, the supervisory authorities and the general public.

[30] Annual reviews: EU–U.S. Privacy Shield – First Annual Joint Review, WP 255, WP29 Report Adopted on 28 November 2017 (hereinafter 'First Joint Review report'); EU-U.S. Privacy Shield - Second Annual Joint Review, EDPB Report Adopted on 22 January 2019 (hereinafter 'Second Joint Review report'); EU-U.S. Privacy Shield - Third Annual Joint Review, EDPB Report Adopted on 12 November 2019 (hereinafter 'Third Joint Review report').
[31] For instance (i) according to the wording of the Draft Decision, Annex I, Section III.6.(f), the DPF Principles would be applicable only where the organisation "stores, uses or discloses" the received data (i.e. not for other operations covered by the term 'processing', such as collecting, recording, alteration, retrieval, consulting, erasure.) and (ii) according to the Draft Decision, Annex I , Section II.4.(a), data security would be imposed only for 'creating, maintaining, using or disseminating' personal information.
[32] Draft Decision, Annex I, I 8.

39. As to the question of diverging interpretations in the EU and the US on the concept of human resources (HR) data, the EDPB agrees with the Commission's third review report on the objective of continuing the discussions with US authorities[33] .

2 GENERAL DATA PROTECTION ASPECTS

2.1 Content principles

2.1.1 Concepts

40. Based on the GDPR Adequacy Referential, basic data protection concepts and/or principles should exist in the third country's legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in European data protection law. For example, the GDPR includes the following important concepts: 'personal data', 'processing of personal data', 'data controller', 'data processor', 'recipient' and 'sensitive data'. The EDPB welcomes that definitions of the terms 'personal data', 'processing' and 'controller' are included in the DPF, as it was the case in the Privacy Shield.

41. The EDPB notes that the extent to which the DPF Principles are applicable to DPF Organisations receiving personal data from the EU for 'mere processing' purposes (referred to as 'agents' or 'processors') remains unclear. The DPF does not distinguish between DPF Principles applicable to agents and DPF Principles applicable to controllers, while several of the obligations included in the DPF Principles are not suitable for agents/processors. For instance, an agent/processor should not be able to provide individuals with all the elements of the full Notice as required by the Notice principle (e.g. the purposes for which it collects and uses personal information about them)[34], as an agent/processor cannot determine alone the means and purposes of the processing[35].

2.1.2 The purpose limitation principle

42. The GDPR Adequacy Referential, in line with the GDPR, provides that personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

43. The Data Integrity and Purpose Limitation principle states that an organisation may not process personal information in a way incompatible with the purposes for which it has been collected or subsequently authorised by the individual[36]. The EDPB notes that different terminology is used under the Notice, the Choice and the Data Integrity and Purpose Limitation principles. As noted by the WP29 and despite useful clarification in the recitals of the Draft Decision, terms such as 'different purposes', 'materially different' purposes, or 'a use that is not consistent with' are used in the DPF without a clear definition of these concepts therein and might lead to legal uncertainty.

[33] Third Joint Review Report, pages. 5, 15-16 and 30; See also Commission Staff Working Document Accompanying the document Report From The Commission to the European Parliament and The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, p.17-18.
[34] Draft Decision, Annex I, Section II.1.(a).
[35] Please also refer to the WP29 Opinion 01/2016, p.16.
[36] Draft Decision, Annex I, Section II.5.

2.1.3 Rights of access, rectification, erasure and objection

44. In the DPF, data subjects' rights to access, rectification and erasure are addressed by the Access principle[37].

45. The Access principle remains unchanged compared to the Privacy Shield. Consequently, some points of concern expressed in the WP29 Opinion 01/2016 are still valid as detailed below.

46. With regard to individuals' right of access, the EDPB finds it necessary to reiterate that the details of the obligation to answer requests from individuals would be better inserted in the main text of the principle (they are still described in a footnote only[38]). Also, it should be clear that access should be provided to the extent that a DPF Organisation processes personal information, not only when it 'stores' it[39]. In the view of the EDPB, the current wording could lead to a narrow interpretation of the right of access.

47. In relation to the list of exceptions to the right of access[40], some still tend to incline the balance towards the interests of DPF organisations. It remains a concern to the EDPB that, in those cases, there seems to be no requirement to take into account the rights and interests of the individual[41].

48. Another exception, which has been subject to previous concern by the WP29[42] and which to the EDPB seems overly broad, is the exception to the right of access for publicly available information and information from public records[43]. The EDPB has repeatedly stated that, according to EU law, data subjects always have the right of access their data regardless of whether or not the personal data have been published. If requests for access were to be rejected on the grounds that the data were obtained from publicly available sources or public records, the individuals would lose the ability to control the accuracy of the data and to control whether the data were lawfully made public in the first place.

49. The EDPB recalls that the right of access is enshrined in Article 8(2) of the Charter. While this is not an absolute right, it is fundamental for the right to the protection of personal data as it facilitates the exercise of the other rights of the data subject, such as correction and erasure, and the right to object[44].

50. In addition to the rights of access, erasure and deletion, data subjects should have the right to object on compelling legitimate grounds relating to their particular situation, at any time, to the processing of their data under specific conditions established in the third country legal framework[45].

51. With the Choice principle, the DPF provides for a right to object (opt-out) to disclosure of personal information to a third party or to the use of personal information for a purpose materially different[46]. In addition, individuals benefit from a right to opt-out to the use of their personal information for direct marketing purpose at any time[47]. Except for the context of direct marketing purposes, the modalities,

[37] Draft Decision, Annex I, II.6 and III.8.a.(i).
[38] Draft Decision, Annex I, III.8.a.(i)1. - footnote 14.
[39] Draft Decision, Annex I, III.8.d(ii).
[40] Draft Decision, Annex I, III.8.e.
[41] WP29 Opinion 01/2016, pt. 2.2.5.
[42] WP29 Opinion 01/2016, pt. 2.2.9.
[43] Draft Decision, Annex I, III.15.d-e.
[44] WP29 Opinion 01/2016, pt. 2.2.5.
[45] GDPR Adequacy Referential, section 3.A.8.
[46] Draft Decision, Annex I, II.2.(a).
[47] Draft Decision, Annex I, III.12.(a).

in particular of the timing, for exercising the right to object, are not detailed. Therefore, the EDPB invites the Commission to clarify how individuals can exercise their right to object.

52. As stated in the WP29 Opinion 01/2016, the EDPB considers that the simple reference to the existence of this right in the privacy policy cannot be sufficient. An individualised opportunity to exercise this right should be offered not only in case of disclosure or re-use of personal information. The EDPB emphasises that a general right to object on compelling legitimate grounds relating to the data subject's particular situation should be offered within the DPF. The EDPB recommends that such right to object be guaranteed at any given moment, and that this right is not limited to the use of the data for direct marketing[48].

53. In relation to HR data, the EDPB appreciates the clarifications of the Commission as regards the application of the Notice and Choice Principles in the situation where a certified U.S. organisation intends to use HR data for a different, non-employment-related purpose, such as marketing communications[49]. However, the EDPB maintains that further processing of HR data for non-employment-related purposes will in most cases be considered incompatible with the original purpose, and that consent will rarely be entirely free when given in an employment context.

54. The EDPB also reiterates the concerns of the WP29 in relation to the exemption to the Notice and Choice Principles for HR data '*to the extent and for the period necessary to avoid prejudicing the ability of the organisation in making promotions, appointments or other similar employment decisions*',[50] which to the EDPB appears broad and vague[51].

2.1.4 Restrictions on onward transfers

55. Onward transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of individuals whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing[52].

56. According to the Accountability for Onward Transfers principle of the DPF, onward transfers can only take place for limited and specified purposes, on the basis of a contract between the DPF Organisation and the third party (or comparable arrangement within a corporate group) and only if that contract requires the third party to provide the same level of protection as the one guaranteed by the DPF Principles[53].

[48] WP29 Opinion 01/2016, pt. 2.2.2.
[49] Draft Decision, Annex I, III.9.b.(i) and Recital 15 and footnote 27.
[50] Draft Decision, Annex I, III.9.b.iv.
[51] WP29 Opinion 01/2016, pt. 2.2.7.
[52] GDPR Adequacy Referential, section 3.A.9.
[53] Draft Decision, Annex I, II.3.

57. The EDPB would like to reiterate the concerns expressed in the WP29 Opinion 01/2016 regarding the exemption to the need of contract for intra-group transfers between controllers[54]. In relation to HR data, the EDPB still does not understand the rationale for the exemption from the obligation to enter into a contract with a third-party controller in case of onward transfers for 'occasional employment-related operational needs'[55].

58. Furthermore, the EDPB would like to repeat the WP29 request[56] that organisations bound by the framework should assess prior to an onward transfer that the mandatory requirements of the third country's national legislation applicable to the recipient would not undermine the continuity of protection of the data subjects whose data are transferred[57].

59. The EDPB maintains that onward transfers of personal data to third countries could lead to interferences with individuals' fundamental rights and invites the Commission to clarify that the safeguards imposed by the initial recipient on the importer in the third country must be effective in light of third country legislation, prior to an onward transfer in the context of the DPF[58] .

2.1.5 Automated decision-making and profiling

60. Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. In the European framework, such conditions include, for example, the need to obtain the explicit consent of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. The law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis[59].

61. The DPF does not provide for any specific legal guarantees where individuals are subject to decisions which produce legal effects concerning or significantly affecting them and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability or conduct.

---

[54] Draft Decision, Annex I, III.10.b(i), which refers to 'or other intra-group instruments (e.g. compliance and control programs') which apparently do not need to be binding.

[55] Draft Decision, Annex I, III.9.e(i), referring to examples such as insurance coverage.

[56] WP29 Opinion 01/2016, pt. 2.2.3, p. 21.

[57] In light of the *Schrems II* judgment, the EDPB has further clarified the obligations for data exporters and importers in relation to onward transfers in a number of guidelines and recommendations: see EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0, adopted on 18 June 2021); Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (Adopted on 10 November 2020); Guidelines 04/2021 on Codes of Conduct as tools for transfers (Version 2.0 Adopted on 22 February 2022); Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Adopted on 14 November 2022); Guidelines 07/2022 on certification as a tool for transfers (adopted after public consultation on 14 February 2023).

[58] WP29 Opinion 01/2016, pt. 2.2.3, p. 21.

[59] GDPR Adequacy Referential, Section 3.B.3.

62. As already considered in the WP29 Opinion 01/2016 and by the EDPB in its previous opinions on the adequacy decisions relating to Japan and South Korea[60], the EDPB finds that rapid developments in the field of automated decision-making and profiling – increasingly by means of AI technologies - call for particular attention in this regard.[61]

63. The EDPB takes note of the Commission's arguments, according to which the absence of specific rules on automated decision-making in the DPF is unlikely to affect the level of protection as regards personal data that has been collected in the Union (since any decision based on automated processing would typically be taken by the controller in the Union which has a direct relationship with the concerned data subject)[62]. However, in the view of the EDPB, it cannot be ruled out that automated decision-making could be used by a US-based controller on data transferred under the Draft Decision (e.g. in the context of employment, for assessing performance at work, insurance, housing).

64. The EDPB welcomes the Commission's references to specific safeguards provided by relevant US law in different fields[63]. However, to the EDPB, the level of protection for individuals appears to vary according to which sector-specific rules – if any – apply to the situation at hand. There is a risk that some situations will not be covered because they do not fall within the scope of the acts referred to. Furthermore, the content of individual rights in relation to automated decision-making is described differently in the various acts.

65. On this background, the EDPB considers that specific rules in the DPF concerning automated decision-making are needed in order to provide sufficient safeguards, including the right for the individual to know the logic involved, to challenge the decision and to obtain human intervention when the decision significantly affects him or her[64].

2.2 Procedural and Enforcement Mechanisms

66. The EDPB notes that the DPF continues to rely on a system of self-certification, even if the Commission refers to it as a system of 'certification'.

67. The EDPB recalls the improvements achieved in the course of the past joint reviews. For instance, as regards the role of the DoC, on the (re-)self-certification process (…), the monitoring of companies' compliance with the DPF Principles (e.g. through spot checks, the use of compliance questionnaires) and identifying and addressing false claims of participation (e.g. through internet searches).

68. At the same time, the WP29 and the EDPB had expressed concerns about a certain lack of oversight of compliance with the requirements of the Privacy Shield[65]. In particular, the EDPB agrees with the Commission's findings after the third annual review of the Privacy Shield that, under the Privacy Shield, spot-checks by the DoC tended to be limited to formal requirements (e.g. lack of response from

[60] EDPB Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, adopted on 5 December 2018; EDPB Opinion 32/2021 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in the Republic of Korea, adopted on 24 September 2021.
[61] See, *inter alia*, C-634/21, *OQ v Land Hesse (SCHUFA Holding and Others)*, Request for preliminary ruling (pending).
[62] Draft Decision, Recitals 33 and 34.
[63] Draft Decision, Recital 35.
[64] See also Third Joint Review report, pt. 76.
[65] Third Joint Review report, pt. 7.

designated points of contact or inaccessibility of a company's privacy policy online)[66]. The EDPB considers that compliance checks as regards more substantive requirements are crucial.

69. The EDPB also recalls the importance of effective oversight (including of compliance with substantive requirements) and enforcement of the DPF. This aspect will be closely monitored by the EDPB, including in the context of the periodic reviews.

70. As regards enforcement, the EDPB takes note of the renewed commitments in the letters from the FTC[67] and the DoT[68] to prioritise the investigation of alleged DPF violations, take appropriate enforcement action against entities making false or deceptive claims of participation, monitor enforcement orders concerning DPF violations and cooperate with EU DPAs. In this respect, the EDPB also recognises that the FTC has indicated that it expects to further focus its enforcement efforts on substantive violations of the DPF and that it intends to investigate (also) on its own initiative. These aspects will be closely monitored by the EDPB including in the context of the periodic reviews.

2.3 Redress mechanisms

71. The EDPB welcomes the clear presentation in the Draft Decision of the seven redress avenues provided to EU data subjects, if their personal data are processed in violation of the DPF[69].

72. These different recourse mechanisms are established in accordance with the requirements of the Recourse, Enforcement and Liability principle and the Supplemental Principle 11 on 'Dispute Resolution and Enforcement' issued by the DoC, and mentioned in Annex I to Draft Decision[70].

73. As underlined by the Commission in its Draft Decision, '*the data subject should be provided with effective administrative and judicial redress*'[71]. This echoes the requirement of Article 45(2)(a) GDPR, according to which the Commission, in its assessment of the adequacy of the level of protection in a third country, has to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'[72]. This requirement is also recalled by the GDPR Adequacy Referential[73].

74. The EDPB notes that these redress mechanisms are the same as those included in the former Privacy Shield, which had been subject to comments by the WP29[74].

75. With regard to the arbitration mechanism, the EDPB notes that this option is not available with respect to the exceptions to the DPF Principles[75] and therefore refers to its comment made in paragraph 33.

[66] Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield (23.10.2019 COM(2019) 495 final), p.4.
[67] Draft Decision, Annex IV
[68] Draft Decision, Annex V
[69] Draft Decision, Recital 67.
[70] Draft Decision, Annex I, Section II.7 and III. 11 and Annex I to Annex I.
[71] Draft Decision, Recital 64.
[72] See also Recital 141 GDPR referring to Article 47 Charter of Fundamental Rights for the right to an effective judicial remedy in the EU.
[73] GDPR Adequacy Referential, p.8.
[74] See in particular, WP29 Opinion 01/2016, Section 2.2.6 (a).
[75] Draft Decision, Annex I to Annex I, A.

76. With regard to additional avenues for judicial redress available under US law, the EDPB would also welcome further details on the legislation mentioned[76] and refer to its comment made in paragraph 21.

77. In addition, the EDPB welcomes the letter from the FTC describing its intent to work closely with EU DPAs[77]. The EDPB also welcomes the prioritisation of complaints by the FTC although it may not give certainty to the data subject that its complaints will be dealt with in all cases.

78. As regards the possibility, in certain cases, for individuals to bring their complaints to an EU DPA, the EDPB would welcome further information (i) as to whether the EU DPA's possibility to give advice on remedial or compensatory measures could include recommendation for fines or the use of investigative powers and (ii) to which extent the EU DPA's action would be taken into account as evidence for enforcement action by the FTC or the DoT[78].

79. The effectiveness of the redress mechanisms will be closely monitored by the EDPB including in the context of the periodic reviews.

3 ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE US

3.1 Access and use for criminal law enforcement purposes

3.1.1 Access by law enforcement authorities to personal data should be based on clear, precise and accessible rules

80. The EDPB welcomes the more detailed information and explanations, compared to the previous adequacy decision, provided for in the Draft Decision with regard to the access and use of personal data by U.S. public authorities for criminal law enforcement purposes. The Draft Decision, in its Annex VI, contains also a letter from the U.S. Department of Justice, Criminal Division "providing a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities". According to the letter, all the legal processes described in the letter are used to obtain information from corporations in the U.S., without regard to the nationality or place of residence of the data subject and stem either from the U.S. Constitution directly (the Fourth Amendment), from statutory and procedural law or from Guidelines and Policies of the Department of Justice. This overview does not cover the national security investigative tools used by law enforcement in terrorism and other national security investigations[79].

81. The EDPB notes that the Draft Decision and its Annex VI discuss primarily federal law enforcement and regulatory authorities[80] and do not refer specifically to the statutes under state law that provide for these procedures to obtain information., Annex VI also mentions that "there are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries

[76] Draft Decision, Recital 85.
[77] Draft Decision, Annex IV.
[78] Draft Decision, Annex I, III.5.b.(iii).
[79] Draft Decision, Footnote 1 to Annex VI.
[80] See Draft Decision, recitals 90-93.

and the types of data they possess", giving in addition several, non-exhaustive examples, such as the Bank Secrecy Act and its implementing regulations[81], the Fair Credit Reporting Act[82], the Right to Financial Privacy Act[83]. The EDPB notes that the applicable legal basis to a given request for access depends on the nature of the data sought, the nature of the company, the nature of the legal procedures (criminal, administrative, related to other public interest) and the nature of the entity requesting access. Since all applicable rules to limit access by law enforcement authorities to data transferred to the U.S. are based on the Constitution, on statutory law and on transparent policies of the Department of Justice, the EDPB acknowledges the accessibility of these rules and invites the Commission to reflect this element in the Draft Decision. It stems from Annex VI, these statutes apply regardless of nationality or place of residence of the data subject and generally incorporate the Fourth Amendment requirements (although they often also go beyond that and include additional protections).

82. In conclusion, the EDPB notes the more detailed assessment contained in the Draft Decision compared to the previous adequacy decision as far as access by federal law enforcement authorities is concerned. As for access by state law enforcement authorities, the EDPB also takes note that according to Annex VI, state law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment. The EDPB invites the Commission to further assess the element of state law protection in the future reviews.

3.1.2 Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

83. The EDPB duly notes that requesting access to data for law enforcement purposes can, in general, be considered to pursue a legitimate objective. However, at the same time, such interferences are only acceptable when they are necessary and proportionate.[84]

84. According to the settled case-law of the CJEU, the principle of proportionality requires that the legislative measures introducing interferences with the rights to private life and to the protection of personal data "be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[85]. Therefore, the assessment of necessity and proportionality is, in principle, always done in relation to a specific measure envisaged by legislation.

85. The U.S. authorities specify in Annex VI that federal prosecutors and federal investigative agents are able to gain access to documents and other record information from organisations through "several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants" and may acquire other communications "pursuant to federal criminal wiretap and

[81] 31 U.S.C. § 5318; 31 C.F.R. Chapter X
[82] 15 U.S.C. § 1681b
[83] 12 U.S.C. §§ 3401-3423
[84] See Judgment of the Court of Justice of 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, ECLI:EU:C:2020:791 (hereinafter, 'CJEU La Quadrature du Net judgment'), paragraph 140. See also EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, 11 April 2017 and EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019.
[85] See Judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (hereinafter: 'CJEU Digital Rights Ireland judgment'), paragraph 46 and case-law cited therein.

pen register authorities"[86]. In addition, agencies with civil and regulatory responsibilities may issue subpoenas to organisations for "business records, electronically stored information, or other tangible items"[87]. The processes themselves are also explained in recitals 90-93 of the Draft Decision. The EDPB notes in this regard a positive development referred to in the Draft Decision in the U.S. jurisprudence regarding the electronically stored information[88].

86. Annex VI furthermore specifies that these legal proceedings are non-discriminatory and used in general to obtain information from 'corporations' in the U.S., irrespective of whether they are certified or not within the U.S.-EU Data Privacy Framework, and "without regard to the nationality or place of residence of the data subject".

87. In addition, Annex VI contains findings regarding the safeguards under the Fourth Amendment of the U.S. Constitution, according to which searches and seizures by law enforcement authorities principally require a court-ordered warrant upon a showing of probable cause and particularity requirements and refers to the fact that in exceptional cases where the warrant requirement does not apply, law enforcement is subject to a reasonableness test under the Fourth Amendment[89]. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial[90].

88. In conclusion, the EDPB notes that the system of investigative tools used to obtain commercial data and other record information from corporations in the U.S. for criminal law enforcement or public interest purposes – including the access limitations and safeguards – provides a comprehensive but also a complex system of measures, reflecting, among other things, the federal nature of the U.S government.

89. Thus, the system of law enforcement investigative measures in the U.S could be considered as generally meeting the requirements of necessity and proportionality in relation to the fundamental rights to private life and data protection.

3.1.3 An independent oversight mechanism should exist

90. The EDPB duly notes the fact that most of the procedures described in the Draft Decision and Annex VI presuppose the involvement of a court's decision before the authorities obtain access to data (e.g. court orders for pen register and trap and races[91], court orders for surveillance pursuant to the Federal Wiretap Law[92], search warrants – Federal Rules of Criminal Procedure, Rule 41[93]). However, it seems that not all of them require the a priori involvement of a court. For instance, civil and regulatory authorities "may issue subpoenas"[94]. In these cases however, there is the possibility of an ex post

[86] Draft Decision, Annex VI, p. 2.
[87] Draft Decision, Annex VI, p. 4.
[88] See Draft Decision, footnote 146. In a 2018 judgment, the U.S. Supreme Court confirmed that a search warrant or warrant exception is also required for law enforcement authorities to access historical cell site location records, that provide a comprehensive overview of a user's movements and that the user can have a reasonable expectation of privacy with respect to such information (Timothy Ivory Carpenter v. United States of America, No. 16-402, 585 U.S. (2018)).
[89] See Draft Decision, Annex VI, p. 2.
[90] See Draft Decision, recital 90.
[91] See Draft Decision, recital 92.
[92] See Draft Decision, Annex VI, p 3.
[93] See Draft Decision, recital 90 and Annex VI, p 3.
[94] See Draft Decision, Annex VI, p. 4 as well as recital 91.

judicial control of the reasonableness of the subpoena, as "a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court"[95].

91. In addition, the Draft Decision describes the oversight of the federal criminal law enforcement agencies by various bodies, from the inner control by the Privacy and Civil Liberties Officers to the external control carried out by the Inspector General and specific Committees in the U.S. Congress[96]. The European Commission provides nuanced and detailed information, and generally reaches comprehensible conclusions. Therefore, the EDPB refrains from reproducing the factual finding and assessments in this opinion.

92. Based on the available information, the EDPB notes that, with regard to access by law enforcement authorities to data held by companies in the U.S., a fairly robust independent oversight mechanism is in place.

3.1.4 Effective remedies need to be available to the individual

93. According to the jurisprudence of the CJEU, an individual must have an effective remedy to satisfy their rights when they consider that they are not or have not been respected. The CJEU explained in Schrems I that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article."[97]

94. The Draft Decision[98] and its Annex VI contain further information with regard to possible remedies stemming from statutory law, which would be available to individuals when public authorities unlawfully obtain access to their data.

95. In this regard, according to the Commission[99], 5 U.S.C. § 702 (Administrative Procedure Act (APA)), provides that a person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof.

96. Furthermore, the Stored Communications Act (SCA) (enacted as title II of the Electronic Communications Privacy Act) provides that, any person aggrieved by any violation of that chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate[100]. In addition, any person who is aggrieved by any willful violation of that chapter or of chapter 119 may commence an action in United States District Court against the United States to recover money damages[101].

[95] See Draft Decision, Annex VI, p. 4 as well as recital 91.
[96] See Draft Decision, Recitals 103-106.
[97] CJEU Schrems I judgment, paragraph 95.
[98] See Draft Decision, recitals 107 to 112.
[99] See Draft Decision, recital 109.
[100] 18 U.S.C. § 2707
[101] 18 U.S.C. § 2712

97. Moreover, the Draft Decision also contains information on the right to obtain access to federal agency records under the Freedom of Information Act (FOIA)[102] and several other statutes which afford individuals the right to bring suit against a U.S. public authority or official with respect to the processing of their personal data, such as the, Wiretap Act, the Computer Fraud and Abuse Act, the Federal Torts Claim Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act[103].

98. The EDPB therefore welcomes the clarifications provided by the Commission as to the number of legal avenues for redress for individuals to rely on. The EDPB also invites the Commission to further clarify whether these remedies allow the data subject to 'have access to personal data relating to him, or to obtain the rectification or erasure of such data' as required by the CJEU.

3.1.5 Further use of the information collected

3.1.5.1 Further use of transferred data accessed by LEA within the US

99. The EDPB positively notes that the Draft Decision assesses the further use of data accessed by law enforcement authorities within the U.S. However, the EDPB regrets that only one example of the grounds on which the information can be further disseminated is given[104]. In that regard, the EDPB recommends the Commission to include further clarification in the Draft Decision on the principles and safeguards applicable on the further use of data, such as those included in the Privacy Act (5 U.S.C. 552a)[105].

3.1.5.2 Onward transfers outside the U.S.

100. The EDPB further notes that the European Commission has also referred to onward transfers from the law enforcement authorities in the U.S to authorities in third countries, but again only with regard to the Attorney General Guidelines for Domestic FBI Operations AGG-DOM[106]. The EDPB considers that such information and assessment are essential in order to allow a comprehensive assessment of the level of protection afforded by the U.S. legislative framework and practices in relation to international disclosure and further use. Given that the Commission has given only one, limited, example regarding the issue of onward transfers outside the U.S. as a whole, the EDPB invites the Commission to further clarify the applicable rules and safeguards for onward transfers, further use and disclosure of personal information, collected for law enforcement purposes in the U.S. and subsequently transferred to third countries, including via international agreements.

3.2 Access and use for national security purposes

101. As a general remark, the EDPB acknowledges that States are granted a broad margin of appreciation in matters of national security, which is also recognised by the ECtHR. The EDPB also recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures[107], Article 6(3) Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence, the latter does not constitute, as long as the EU has not acceded to it, a legal instrument which has

[102] See Draft Decision, recital 111.
[103] See Draft Decision, recital 112.
[104] See Draft Decision, recital 102.
[105] See Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), page 36, p. B (1)(g)
[106] See Draft Decision, recital 102.
[107] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

been formally incorporated into EU law[108]. Thus, the level of protection of fundamental rights required by Article 45 GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the EU Charter. This being said, according to Article 52(3) EU Charter, the rights contained therein that correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights that are also foreseen in the EU Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the EU Charter[109]. According to the last sentence of Article 52(3) EU Charter, however, *"[t]his provision shall not prevent Union law providing more extensive protection*."

102. Therefore, in the following assessment, the EDPB has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law.

103. Several legal instruments provide for the possibility to collect and further access and process data for U.S. Intelligence agencies in the U.S. legal framework.

104. As recalled by the European Commission in its Draft Decision, "*U.S. intelligence agencies may seek access to personal data that has been transferred to organisations located in the United States for national security purposes only as authorised by statute, specifically under the Foreign Intelligence Surveillance Act (FISA) or and statutory provisions authorising access through National Security Letters (NSL)*"[110]. "*U.S. intelligence agencies also have possibilities to collect personal data outside the United States, which may include personal data in transit between the Union and the United States"* under the Executive Order 12333 (EO 12333)[111].

105. With respect to the specific data collection regimes, in particular Section 702 FISA and EO 12333, EO 14086 now provides for new rules to enhance safeguards for the United States Signals Intelligence Activities. These general rules apply horizontally and "*must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations*"[112]. The EO 14086 has mostly replaced the previous Presidential Policy Directive 28 ('PPD-28')[113].

106. In order to assess the legal framework applying to collection, access and further processing of data for national security purposes, it is thus important to examine the specific legal framework governing the collection of data within and outside the U.S., i.e. Section 702 FISA and EO 12333, which, as such, have not changed since the previous review of the Privacy Shield, taking into account the fact that the new Executive Order 14086 provides safeguards to be implemented also in the context of collection of data on the ground of specific texts such as Section 702 FISA and EO 12333.

[108] See CJEU Schrems II judgment, para. 98.
[109] See CJEU La Quadrature du Net judgment, para. 124.
[110] See Draft Decision, recital 115.
[111] See Draft Decision, recital 117.
[112] See Draft Decision, recital 120.
[113] This Executive Order revokes PPD-28 except for sections 3 and 6 of that directive and the classified annex to that directive, which remain in effect. See presidential national security memorandum of 7 October 2022.

3.2.1 Guarantee A - Processing should be in accordance with the law and based on clear, precise and accessible rules

107. For its assessment of the general setup of data collection for the purpose of national security, the EDPB wishes to recall the first of the four so called "European essential guarantees", according to which 'processing should be based on clear, precise and accessible rules' [114].

108. In accordance with the settled case law of the CJEU, 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[115]. The Court also recalled that "legislation must be legally binding under domestic law"[116]. In this regard, the ECtHR case-law clarifies that the term 'law' should be understood in its substantive sense, not its formal one. It may include enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament and even unwritten law. To be 'law', a norm must at least be adequately accessible and formulated with sufficient precision[117].

109. The degree of precision required must be measured in relation to the extent of the limitation of the right[118]. Furthermore, as regards 'foreseeability' of the law, the ECtHR recalled in *Zakharov* that in the context of secret measures of surveillance, such as the interception of communications, "foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly". However, clear and detailed rules on secret surveillance measures are essential to prevent the risks of arbitrariness where a power vested in the executive is exercised in secret. "The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"[119].

110. In addition, the CJEU clarified that the assessment of the applicable third country law should focus on whether it can be invoked and relied on by individuals before a court. The rights granted to data subjects should notably be actionable and individuals have to be provided with enforceable rights against public authorities[120], which was not the case in the context of the previous PPD-28. The EO 14086, which, the EDPB understands, is deemed to have the same legal effect within the US legal order as PPD-28 (i.e. binding on the executive), now provides for actionable entitlements against public authorities. A detailed assessment of the new enforceable rights of the data subjects is provided in the section on redress.

111. Recitals 114-152 of the Draft Decision and Annex VII provide a summary of some aspects of the governing legal framework, the collection limitations, the retention and dissemination limitations, compliance and oversight, transparency and redress. The U.S. legal system for intelligence activities

[114] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020. See §175 and §180 Schrems II and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, § 139 and the case-law cited.
[115] See CJEU Schrems II judgment, paragraphs 174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 Privacy International ECLI:EU:C:2020:790 (hereinafter, 'CJEU Privacy International judgment'), paragraph 65; and CJEU La Quadrature du Net judgment, paragraph 175.
[116] CJEU Privacy International judgment, paragraph 68.
[117] ECtHR, Sunday Times v UK (No 1), 26 April 1979, CE:ECHR:1979:0426JUD000653874 (hereinafter, 'ECtHR Sunday Times v UK No 1 judgment'), para 49.
[118] ECtHR Sunday Times v UK No 1 judgment, para 49.
[119] ECtHR, Zakharov v. Russia, 4 December 2015 (hereinafter, 'ECtHR Zakharov judgment'), paragraph 229.
[120] CJEU Schrems II judgment, paragraph 181.

consists of a number of different documents including individual agencies reports, policies and procedures. In that regard, the EDPB evaluation is focused on a limited number of issues that it considers crucial.

112. According to recitals 115 to 119 of the Draft Decision, access to transferred personal data by US national security authorities may only take place under FISA, under other statutory provisions (12 U.S.C. §3414, 15 U.S.C. § 1681u-1681v and 18 U.S.C. § 2709) or, in connection with personal data in transit, on the basis of EO 12333. It stems from recitals 116 and 118 of the Draft Decision that the Commission focuses its assessment, in connection with access to personal data by US national security authorities, on sections 105, 302, 402, 501 and 702 FISA (foreign intelligence activities targeting non-US persons located outside the US) and EO 12333 (foreign intelligence activities on personal data in transit), as being the most relevant. The EDPB opinion is therefore limited to the assessment of these provisions made by the Commission, taking into account the limitations and safeguards set out in EO 14086[121].

113. In this respect, it is to be noted that all legal instruments mentioned in the Draft Decision are accessible for the general public (in and outside of the U.S.) and available online. Furthermore, the requirements laid down in the EO are binding on the entire Intelligence Community[122] and apply in a cross-cutting way to all foreign intelligence purpose activities.

114. The concept of 'signals intelligence' is not defined in the EO 14086. The latter refers to the definitions set out in the EO 12333 for establishing the scope of foreign intelligence and counterintelligence, which are defined broadly. In this regard, even if it has been argued that since the introduction of FISA, EO 12333 can only be used for the collection of data outside the U.S. territory, the EDPB recalls that EO 12333 itself, which remains intact, lacks of sufficient details regarding its geographical scope, the extent to which data can be collected, retained or further disseminated, or on the nature of offences that may give rise to surveillance or the kind of information that may be collected or used. In principle, all foreign intelligence data collection within the scope of EO 12333 can take place at the discretion of the U.S. President.[123] However, in the understanding of the EDPB, the main purpose of the EO 14086 is to prescribe the limits for the collection and the processing of personal data in the context of foreign intelligence, no matter which surveillance programme is used and where data is obtained from. It is therefore the understanding of the EDPB that the additional safeguards provided for under EO 14086 also apply in the context of surveillance programmes applicable to personal data in transit taking place under EO 12333[124].

115. In this respect, the EO 14086 lists 12 legitimate objectives that should be pursued when conducting signals intelligence collection and 5 objectives for which signals intelligence collection must not be conducted[125], as well as 6 legitimate objectives for the use of data collected in bulk[126]. While some of them are quite detailed (e.g. 'rescue of hostages'), some others are more general (e.g. 'global security'). The EO 14086 sets out also a list of prohibited objectives, which includes notably the

121 This Executive Order revokes PPD-28 except for sections 3 and 6 of that directive and the classified annex to that directive, which remain in effect. See presidential national security memorandum of 7 October 2022
122 See Draft Decision, recital 120.
123 Under Article II of the U.S. Constitution, responsibility ensuring national security including in particular gathering foreign intelligence falls within the President's authority as Commander in Chief of the armed forces.
124 See Draft Decision, recital 134.
125 See Executive Order 14086 ('EO 14086'), section 2, (b), (ii), A, 1 to 5.
126 See Draft Decision, recital 134 and EO 14086, section 2(c)(ii).

suppression or restriction of 'legitimate privacy interests'[127]. The EO 14086 also provides for the possibility for the President of the United States to add other objectives to the list for which collection is allowed, which could, upon decision of the President, not be released to the public if the President considers that doing so would pose a risk to the national security of the United States[128]. Such updates may only be authorised 'in light of new national security imperatives'.

116. The objectives cannot by themselves be relied upon by intelligence agencies to justify signals intelligence collection but must be further substantiated, for operational purposes, into more concrete priorities for which signals intelligence may be collected. The EO 14086 details the procedure for the validation of the priorities for which signals intelligence may be collected[129]. The EDPB understands that the process to define the validated intelligence priorities in principle relies on the Director of the Intelligence Community and acknowledges that it should as a rule involve the assessment of the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO), with which the Director can disagree, in which case it "shall include the CLPO's assessment and the Director's views when presenting the National Intelligence Priorities Framework (NIPF) to the President"[130].

117. However, the EDPB also notes that according to the definition of "*validated intelligence priority*", such priorities mean for "*most United States signals intelligence collection activities*"[131] a priority validated under section 2(b)(iii) of the EO (described in the previous paragraph). The process of validation can in some cases differ from this process in "*narrow circumstances*", in which case, the President or the head of an element of the Intelligence Community may set a priority, "*to the extent feasible*" in accordance with the criteria set by the same section 2(b)(iii)(A)(1)-(3), which includes the requirement for appropriate consideration for the privacy and civil liberties of all persons, but without the involvement of the CLPO.

118. The EO 14086 in addition underlines that 'signals intelligence collection activities shall be as tailored as feasible' to advance a validated intelligence priority, and that 'the Intelligence Community shall consider the availability, feasibility, and appropriateness of other less intrusive sources' and provides general necessity and proportionality requirements[132].

119. Furthermore, according to Section 5(h), EO 14086 creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO's decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of that Order.

120. The text of FISA appears to be clearer and more precise than EO 12333 on the kind of intelligence operations that can be mandated. FISA and EO 12333 now have to be applied in the light of EO 14086 and in particular taking into account inter alia the principles of necessity and proportionality.

121. The requirements laid down in the EO 14086 must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations. In this respect, EO 14086 provides U.S. intelligence agencies with a maximum of one year to update their existing policies and procedures (i.e. by 7 October 2023) to bring them in line with the EO's requirements. Such updated policies and procedures have to be developed in consultation with the Attorney General, the

[127] See EO 14086, Section 2(b)(ii)(A)(2).
[128] See EO 14086, Section 2(b)(i)(B).
[129] See Draft Decision, recital 129.
[130] See EO 14086, section 2(b)(iii)(B).
[131] See EO 14086, Section 4, (n)
[132] See EO 14086, Section 2(c)(i) (A) and (B).

CLPO and the Privacy and Civil Liberties Oversight Board (PCLOB) and be made publicly available to the maximum extent possible[133].

122. The EDPB would welcome that not only the entry into force but also the adoption of the decision are conditional upon inter alia the adoption of updated policies and procedures to implement EO 14086 by all US intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share this assessment with the EDPB.

123. Finally, in relation to the retention of the transferred data once collected for national security purposes, the EDPB notes that the EO 14086 ensures that the rules applicable to personal data of US persons are also applicable to non-US persons' personal data[134]. From the Draft Decision, it appears that these rules are provided for in section 309 of the Intelligence Authorization Act for Fiscal Year 2015[135], which establishes a maximum retention period of 5 years in principle of any non-public telephone or electronic communication acquired without the consent of the person. The EDPB recommends in this regard that the Commission provide more clarity as to its assessment of the retention rules applicable to personal data of US persons in the decision.

3.2.2 Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

3.2.2.1 Horizontal safeguards provided by the new Executive Order 14086 – Necessity and proportionality

124. The new EO 14086 which generally replaces PPD-28, aims at providing rules to enhance safeguards for United States Signals Intelligence Activities, to be further implemented by the Intelligence Community elements in their internal policies and procedures.

125. EO 14086 introduces two new requirements under US law which echo the requirements recalled by the CJEU in its Schrems II judgment, namely that signals intelligence activities shall be conducted only as far as necessary to advance a validated intelligence priority collection and only to the extent and in a manner that is proportionate to the validated intelligence priority[136].

126. It is the understanding of the EDPB that these elements have been included to reflect the principles of necessity and proportionality foreseen under EU law and in the CJEU and ECHR case-law which aim at ensuring that collection and processing of data should be limited to what is necessary and proportionate.

127. In this regard the EDPB recalls the process foreseen for the validation of intelligence priorities as well as the possible derogation (see paragraphs 116, 117).

128. Furthermore, the EDPB notes that these principles of necessity and proportionality provided in the EO will have to be operationalized and implemented, within one year, in the policies and procedures of each element of the Intelligence Community[137].

[133] See EO 14086, Section 2(c)(iv)(B) and (C).
[134] Draft Decision, recital 150.
[135] Draft Decision, footnote 272.
[136] See EO 14086, Section 2, (a), (ii), A and B.
[137] See EO 14086, Section 2, (c), (iv), B

3.2.2.2 Specific safeguards for the collection of signals intelligence

129. The EDPB also notes that EO 14086 provides for limitations regarding the objectives for which personal data can and cannot be collected, in the context of collection of signals intelligence[138].

130. The EDPB welcomes that the EO provides that targeted collection should be prioritized over bulk collection[139]. In the context of collection of signals intelligence, the EO provides for a list of 12 objectives for which data can be collected, which have to be further substantiated into intelligence priorities (see paragraph 117), as well as a list of 5 objectives for which signals intelligence collection activities shall not be conducted[140]. In principle these provisions constitute a guarantee to ensure the necessity of the collection of data.

131. Yet, the EDPB recalls that EO 14086, also provides for the possibility for the President of the United States to add other objectives to the list (see paragraphs 114, 115).[141]

3.2.2.3 Specific safeguards for bulk collection

132. The CJEU underlined in its Schrems I judgment that the "*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*"[142] and ruled that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*".

133. In the Schrems II case[143], with regards to its analysis of bulk collection in relation to the correlated reading of EO 12 333 and PPD-28, and in particular points 183 to 185, the Court stressed, as recalled above, that the possibility of bulk collection, « *which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data*. ».

134. The EDPB thus notes that the CJEU did not exclude, by principle, bulk collection, but considered in its Schrems II decision that for such bulk collection to take place lawfully, sufficiently clear and precise limits must be in place to delimit the scope of such bulk collection.

135. The EDPB also recognizes that while replacing the PPD-28, the EO 14086 provides for new safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. laws do not apply.

136. With regards to bulk collection of data, the EDPB takes note that the EO 14086 provides that bulk collection continues to be permitted. Indeed, the EDPB underlines that the definition of bulk collection remains the same as in the previous PPD-28: "*signals intelligence collected in 'bulk' means the authorised collection of large quantities of signals intelligence data which, due to technical or*

[138] See EO 14086, section 2, (b), (i), A, 1 to 12
[139] See EO 14086, section 2, (c), (ii), A
[140] See EO 14086, section 2, (b), (ii), A, 1 to 5
[141] See EO 14086, section 2, (b), (i), B
[142] CJEU Schrems I judgment, para 92.
[143] See CJEU Schrems II judgment.

operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms.)"[144].

137. Since the Schrems II ruling, the Court did not detail precisely the safeguards required for bulk collection to take place. However, the EDPB recalls that the ECHR has issued important decisions concerning bulk collection and the relevant safeguards in this context.

138. The EDPB recalls that bulk collection, by allowing for the collection of large quantities of data without discriminant presents higher risks for the individuals[145] than targeted collection and thus requires additional safeguards to be adduced.

139. The EDPB also notes that the CJEU has developed further case law concerning retention of traffic and location data, and subsequent access to these data retained by telecommunications operators, including for national security purposes, which, although they cannot be deemed directly applicable in this context, to some extent could be relevant in the context of the present assessment of bulk collection in the context of EO 12333.

1) <u>Purpose limitation</u>

140. The EO provides that bulk collection should take place only following a determination that « *the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection* »[146], and that « *the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information* »[147]. In addition to these safeguards, the EDPB also recognizes that the use of data collected in bulk shall be used in pursuit of one or more of the six objectives listed[148]. The EDPB further stresses that while these objectives are more detailed than those which were provided in the previous PPD-28, generally replaced by EO 14086, the scale of such collection possibilities remains potentially broad, i.e. encompassing large volumes of data.

141. The EDPB here as well recalls that EO 14086, also provides for the possibility for the President of the United States to add other objectives to the list (see paragraph 115)[149].

2) <u>Prior independent authorisation</u>

142. The EDPB stresses that the ECtHR dedicates a significant importance to prior independent authorization in the context of bulk collection of data for national security purposes. Indeed the Court ruled in particular that "*in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent*

[144] See EO 14086, Section 4, (b)
[145] See for instance ECtHR (Grand Chamber), Big Brother Watch and others v. The United Kingdom, 25 May 2021 (hereinafter, 'ECtHR Big Brother Watch judgment'), recital 363, where the Court indicates that it "*is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content*".
[146] EO 14086, Section 2(c)(ii)(A).
[147] EO 14086, Section 2(c)(ii)(A).
[148] EO 14086, Section 2(c)(ii)(B).
[149] See EO 14086, Section 2(c)(ii)(C).

authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime."[150]

143. The EDPB also notes the following paragraph of this judgment in Grand Chamber, where the Strasbourg Court further highlights that it "*agrees with the Chamber that while judicial authorisation is an* "*important safeguard against arbitrariness" it is not a "necessary requirement" (see paragraphs 318-320 of the Chamber judgment). Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive*"[151].

144. In this context, the EDPB notes that the EO does not provide for such independent prior authorization for bulk collection, and that this is not foreseen as well under EO 12333 (see section below on EO 12333).

3) <u>Retention rules</u>

145. The EDPB recalls that another important set of safeguards are the rules for the duration of the collection and retention of data. In this respect, the ECtHR stressed that "*domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed*"[152] as these safeguards "*are equally relevant to bulk interception*."[153]

146. In this regard, it is the understanding of the EDPB that the EO provides for rules concerning the retention of data for personal data collected through signals intelligence, including in bulk[154]. The EDPB notes that, according to Section 2(c)(iii)(A) of EO 14086, each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence. However, these rules do not provide for a specific retention period but rather refer in general to the same applicable rules for the retention of data concerning US persons and to situations where no final retention determination has been made. The EDPB is thus concerned that these retention periods, as for targeted collection (see paragraph 122), are not clearly defined in this EO with regards to data collected in bulk. It calls on the Commission to share its assessment on the necessity and proportionality of the retention periods applicable to US persons and the available information concerning retention periods in practice where no final retention determination has been made under US law, as in its current state, the Draft Decision merely recalls this general rule in a single short paragraph[155] and a footnote[156] which does not allow to determine whether these retention periods are necessary and proportionate. Since, as underlined by the ECtHR, this is a crucial safeguard for data subjects to be able to exercise their rights in a context where a particularly intrusive measure is taken to collect their data in the first place, the EDPB calls on the

[150] See ECtHR Big Brother Watch judgment, para. 350.
[151] See ECtHR Big Brother Watch judgment, para. 351.
[152] See ECtHR Big Brother Watch judgment, para. 348.
[153] See ECtHR Big Brother Watch judgment, para. 348.
[154] See EO 14086, section 2, (c), (iii), A, (2)(a)-(c).
[155] See Draft Decision, para. 150.
[156] See Draft Decision, footnote 271.

European Commission to provide further clarifications concerning the different retention periods in practice.

4) Safeguards concerning "dissemination"

147. Also, the EDPB recalls that to ensure the effectivity of necessity and proportionality and the purpose limitation principle, the ECtHR also recognized the importance of rules provided by law concerning the further dissemination of the data collected, including in context of bulk collection[157].

148. Section 2(c)(iii)(A)(1)(c) of EO 14086 provides that information about non-U.S. persons that was collected through signals intelligence activities may only be disseminated if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information.

149. Taking this into account, the EDPB understands that the provisions concerning dissemination under the EO 14086 do not provide neither for an express prohibition of dissemination for other purposes than national security purposes when dissemination to US competent authorities is concerned[158]. The EDPB calls on the Commission to further clarify the applicable rules and safeguards in this case.

150. The EDPB is therefore concerned that data acquired by the competent Intelligence Community authorities could then be disseminated to US competent authorities for the purpose of combating crime, including serious crimes, in the context of criminal investigations, thereby providing law enforcement authorities, without any further specific restrictions, with a possibility to obtain data that they would have been prohibited from collecting directly and calls on the Commission to further assess this point.

151. In the specific context of onward transfers (dissemination to recipients outside the United States Government, including to a foreign government or international organization[159]), the EDPB recalls that it is of the view that the protection afforded to data should also be maintained in the context of onward transfers including in the field of national security[160].

152. In this respect, the EO provides for some safeguards, namely the requirement to take due account of the purpose of the dissemination – although without expressly requiring that the purpose of dissemination should also be for the protection of national security – the nature and the extent of the personal information being disseminated and the potential harmful impact on the person or persons concerned before disseminating the data.

153. While the EDPB acknowledges that some of these safeguards, in particular the account to be given to the "*potential for harmful impact*"[161] on the data subject(s) concerned, reflect some requirements of the ECHR, it also stresses that the Strasbourg Court furthermore requires that a legally binding obligation "*to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards*"[162], which the EDPB does not expressly find in the provisions of the EO

[157] See ECtHR Big Brother Watch judgment, para. 348.
[158] See EO 14086, Sec 2.(c)(iii)(A)(1).
[159] See EO 14086, Sec 2.(c)(iii)(A)(1), (d) in particular.
[160] See for instance EDPB Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. Adopted on 13 April 2021, sections 4.3.2.1 and 4.3.2.2.
[161] See EO 14086, Sec 2.(c)(iii)(A)(1), (d)
[162] See ECtHR (Grand Chamber), Case of Centrum För Rättvisa V. Sweden, 25 May 2021, para 326.

relating to dissemination to foreign recipients. The EDPB invites therefore the Commission to further assess this element.

154. The EDPB also notes that the European Commission did not consider, as part of its adequacy assessment, the existence of international agreements concluded with third countries or international organisations that may provide for specific provisions for the international transfer of personal data by intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of intelligence cooperation are likely to affect the data protection legal framework as assessed.

155. The EDPB therefore invites the European Commission to clarify whether such agreements exist, under which conditions they may be concluded and assess whether the provisions of international agreements may affect the level of protection afforded to personal data transferred from the EEA by the legislative framework and practices in relation to onward transfers for national security purposes.

5) Temporary bulk collection to support the initial technical phase of targeted collection

156. The EDPB recalls that, in the context of the last Joint Review of the Privacy Shield, discussions mainly focused on the interpretation and application of the additional ground (situation/scenario) for bulk collection foreseen by the first sentence of footnote 5 of Section 2 PPD28-, which provided that "*The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection*." The U.S. authorities explained at the time the meaning of "*signals intelligence data that is temporarily acquired to facilitate targeted collection*". The EDPB understood from these discussions that this footnote meant that data may be collected in bulk - and regardless of the six purposes foreseen - if collected temporarily, with a view to establishing an identifier for a defined target. This would thus be an additional ground to collect data in bulk, and in this case only the general principles of Section 1 of PPD-28 would have still applied. As recalled above, in the Schrems II ruling, the CJEU considered that the combined EO 12333 and PPD-28 with regards to bulk collection did not "*delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data"*[163]*.*

157. The EDPB notes that a derogation allowing for such kind of bulk collection is still provided in the EO 14086[164]; however, the EDPB welcomes that this derogation has been narrowed compared to PPD-28 and additional safeguards are provided under the EO 14086.

158. The EDPB understands that the new EO 14086 provides for safeguards which remain applicable in the context of this type of temporary technical bulk collection, in particular the general principles of necessity and proportionality in relation to the validated intelligence priority when data are acquired without discriminants before targeted collection takes place (Section 2(a)-(b), Section 2(c)(i) EO 14086). It is also the understanding of the EDPB that such bulk collection supporting a subsequent targeted signals intelligence collection is also subject to the additional safeguards provided from subsection (2)(c)(iii) onwards[165].

159. However, the EDPB also recalls – see above paragraph 117 – that the definition of "*validated intelligence priority*" provides for a derogatory procedure which would not involve the CLPO of the Office of the Director of National Intelligence.

[163] CJEU Schrems II judgment, paragraph 183.
[164] See EO 14086, section 2 (c), (ii), D and Draft Decision, footnote 226.
[165] See previous sections for further elements on these provisions.

160. However, the EDPB still notes that the safeguards of the subsection concerning bulk collection do not apply to temporary bulk collection used to support the initial technical phase of targeted signals intelligence collection activity as outlined in Section 2(c)(ii)(D) of EO 14086, which notably means that in this context data collected in bulk can be used for other purposes than those listed under subsection 2 (c)(ii). The EDPB would welcome clarifications in the Draft Decision on the purposes for which data collected in bulk in this context can be used as well as concerning the application of the limitations set out under subsection 2(c)(i) for the collection of signals intelligence in general (namely only for the legitimate objectives listed there) in the context of temporary bulk collection in the Draft Decision.

161. To conclude, the EDPB also stresses that this derogation for temporary bulk collection in view of targeted collection and the remaining safeguards to be applied remains unclear, in particular as to which safeguards of the EO 14086 would apply to which stage (bulk collection, further targeted collection) and calls on the Commission to further assess these elements, and assess these aspects also in practice in the future joint reviews.

162. Furthermore, although the EDPB also further regrets that even if the notion of "temporarily" has been slightly more detailed in the EO than in the PPD-28, in the EDPB's understanding, it still appears to mean that as long as the target has not been identified, bulk collection could continue. In this regard, the EDPB recalls the necessity to have clear and precise rules and stresses here as well the key safeguard that these rules constitute for data subjects.

163. In conclusion, concerning the safeguards applicable to bulk collection, the EDPB remains concerned that, despite additional safeguards provided under EO 14086, the possibility to collect data in bulk, i.e. without discriminants, is still provided, without key safeguards such as prior authorisation to collect these data - including in the derogatory situation of temporary technical bulk collection -, also taking into account the need for further clarifications and the concerns expressed regarding strict purpose limitation to access the data subsequently, clear and strict data retention rules and stricter safeguards concerning dissemination of data collected in bulk, including in the context of onward transfers.

164. In general, the EDPB stresses that the above-mentioned decision of the ECtHR, once again show the importance of comprehensive supervision by independent supervisory authorities. The EDPB emphasizes that independent oversight at all stages of the process of government access for national security purposes is an important safeguard against arbitrary surveillance measures and thus for the assessment of an adequate level of data protection. The guarantee of independence of the supervisory authorities within the meaning of Article 8(3) of the Charter is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data. This applies in particular in circumstances where, due to the nature of secret surveillance, the individual is prevented from seeking review or from taking a direct part in any review proceedings prior or during the execution of the surveillance measure.

165. The EDPB recalls that it is of the opinion that the assessment of adequacy depends on all the circumstances of the case, in particular on the effectiveness of ex post oversight and legal redress as provided for in the legal framework.

3.2.2.4 Legal framework organizing specific collection for national security purposes by the IC elements within and outside the U.S. territory

166. In its Schrems II ruling, the CJEU stressed, in relation to Section 702 FISA that this text "*does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those*

programmes"[166]. It led the Court to consider that "*in those circumstances (…), that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter (…), according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*"[167].

167. In relation to EO 12333, the Court noted that it "*does not confer rights which are enforceable against the US authorities in the courts*"[168] and also concluded that "*in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data*"[169], following the analysis of the conditions under which bulk collection could take place under this order, in conjunction with PPD-28.

168. With respect to these specific data collection regimes, EO 14086 now provides for new rules.

3.2.2.4.1 Collection of data for national security purposes under Section 702

169. The EDPB recalls that the findings on FISA 702[170] that "*in practice, 'non-U.S. persons' also benefit from the access and retention restrictions required by the different agencies' minimisation and/or targeting procedures due to the cost and difficulty of identifying and removing U.S person information for a large body of data means that typically the entire data set is handled in compliance with the higher U.S data standards*" were welcomed in the PCLOB last report.

170. According to those findings, "*the programme does not operate by collecting communications in bulk*". The 2014 and 2021 Statistical Transparency Reports issued by the ODNI confirmed this finding. Additionally, according to PCLOB report, "tasked selectors", such as an e-mail address or a telephone number, are used to target the surveillance.

171. Yet, the EDPB also recalls that, at the same time, in the context of Section 702, it was clarified during the last Review of the Privacy Shield that a "person" to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals would be non-U.S. persons and fulfill the applicable criteria for being targeted. Also the EDPB recalls that during the Third Annual Joint Review of the Privacy Shield in 2019 further clarification in the context of the UPSTREAM program was called upon to exclude that massive and indiscriminate access to personal data of non-U.S. persons take place[171].

172. Moreover, the EDPB recalls that the fact that the collection under section 702 FISA is justified by "a *significant purpose of the acquisition is to obtain foreign intelligence information*" still leaves some uncertainty regarding its purpose limitation and necessity. The EDPB notes however that according to EO 14086, section 2(a)(A) and (B), signals intelligence activities shall be conducted only following a determination that the activities are necessary to advance a validated priority and only to the extent and in a manner that is proportionate to such priority and that it shall be as tailored as feasible to advance the validated priority, taking due account of relevant factors such as the intrusiveness of the

[166] See CJEU Schrems II Judgment, para 180.
[167] See CJEU Schrems II Judgment, para 180.
[168] See CJEU Schrems II Judgment, para 182.
[169] See CJEU Schrems II Judgment, para 183.
[170] See PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, page 100.
[171] See Third Joint Review report, page 17, para 83.

collection, the sensitivity of the data, not disproportionally impact privacy and civil liberties. The EDPB yet expects further clarifications as to how this will be concretely implemented and operationalized, including in the context of the application of FISA Section 702.

173. In this regard, in the absence of direct access to this information by itself, the EDPB called for an independent assessment on the necessity and proportionality of the definition of "targets" and of the concept of "foreign intelligence" under section 702 FISA (including in the context of the UPSTREAM program) following its renewal. The EDPB considers that its previous call for further independent assessment of the process of application of selectors in specific cases ("tasking of selectors") as well as for further clarification in the context of the UPSTREAM program is relevant. Therefore, taking into account the new EO 14086, the EDPB calls for additional information in order to also assess and monitor how and to which extent the newly introduced principles of necessity and proportionality will be applied in practice in this context and expects that this will also be assessed in the context of future joint reviews.

174. The EDPB welcomes that the fully functional Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency, has decided to conduct "an Oversight Project to examine the surveillance program that the Executive Branch operates pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA), in anticipation of the December 2023 sunset date for Section 702 and the upcoming public and Congressional consideration of its reauthorization"[172]. The EDPB also welcomes that the "review covers selected focus areas for investigation, including but not necessarily limited to, U.S. Person queries of information collected under Section 702, and 'Upstream' collection conducted pursuant to Section 702"[173] and "also includes reviewing the program's past and projected value and efficacy, as well as the adequacy of existing privacy and civil liberties safeguards"[174]. The EDPB consequently stresses that access to the findings of the PCLOB in this report on section 702 would be necessary to adequately and comprehensively assess the privacy safeguards provided and applied in the context of this surveillance program.

175. Taking into account the new EO 14086, the EDPB additionally calls for additional information in order to also assess and monitor how and to which extent the newly introduced principles of necessity and proportionality, as well as the other safeguards provided in this text will be applied in practice in this context.

3.2.2.4.2 Collection of data for national security purposes under Executive Order 12333

176. As recognized by the CJEU in its Schrems II ruling, the analysis of the laws of the third country for which adequacy is considered, should not be limited to the laws and practices allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal data "in transit" to the country, for which adequacy is recognized.

177. The EDPB welcomes the general public report issued by the PCLOB on the Executive Order 12333 and released in April 2021, but notes that this report remains general as most of the findings are classified.

---

[172] See the NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)
[173] See above.
[174] See above.

178. In this context, once again, given the uncertainty and lack of clarity on how EO 12333 used to be applied, and the importance of clarifying how it will be applied in light of the new EO 14086, the EDPB stresses the importance of the awaited PCLOB's reports on this text[175]. However, it understands that most of their content is likely to remain classified, so that no further information on the concrete operation of EO 12333 and on its necessity and proportionality would become available neither to the public, nor to the EDPB.

179. The EDPB therefore would particularly welcome the report of the PCLOB on the application of the EO 14086 not being classified but fully accessible once it is completed, including on the parts which would assess how the EO 14086's safeguards will be applied to collection of data under EO 12333. The EDPB also invites the Commission to be specifically attentive to this point in the context of the future joint reviews.

180. In general, with regards to the different legal instruments providing for the possibility to collect and further access and process data for U.S. Intelligence agencies in the U.S. legal framework, the EDPB would welcome clarifications as to their interplay with the new EO 14086 and expects assurances that the previous concerns expressed in the previous opinions of the EDPB in their regards would be resolved by the adoption of these new safeguards.

181. The EDPB also calls on the Commission to be specifically attentive to these aspects in the context of future joint reviews.

3.2.2.4.3 PCLOB report

182. The EDPB welcomes that EO 14086 also provides for the requirement for the PCLOB to produce a report concerning the implementation of the EO. The EDPB stresses that this report should include an assessment of this specific possibility provided by the EO to collect data, for the purposes listed for targeted collection, as well as in bulk, including for technical reasons, in order to better understand the key terms of the EO 14086 and how they are practically understood and applied in the different surveillance programs. This report would also be necessary to assess how the EO will be implemented in the internal procedures and policies of the IC elements.

3.2.3 Guarantee C - Oversight

3.2.3.1 Introduction

183. The U.S. intelligence activities are subject to a multi-layered oversight process. The oversight structure in the U.S. can be divided in internal and external oversight. All intelligence community elements have oversight and compliance officials, which conduct periodic oversight of signals intelligence activities, including Privacy and Civil Liberties Officers and Inspectors General. In addition, there are external oversight bodies, such as the Privacy and Civil Liberties Oversight Board (PCLOB) and the Intelligence Oversight Board.

184. The EDPB recalls that an interference takes place at the time of collection of the data, but also at the time the data is accessed by a public authority for further processing. The ECtHR has specified multiple

[175] The general report on EO 12333 has remained mostly classified - only a short public version has been made public, as well as the report and Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O. 12333, as well only partly declassified.

times that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[176] (e.g. an administrative authority or a parliamentary body).

185. While the ECtHR has expressed its preference for a judge to be responsible to maintain oversight, it did not exclude that another body may be responsible, "*provided that the authority is sufficiently independent from the executive*"[177] and "*of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control*".[178]

186. The ECtHR added that "*the manner of appointment and the legal status of the members of the supervisory body*"[179] need to be taken into account when assessing independence.

187. The ECtHR also stated, that it is to examine, whether the supervisory body's activities are open to public scrutiny. For example, this could be accomplished, where the supervision reports annually to the government, respectively the public reports are laid before Parliament and were discussed by Parliament.[180]

188. The independent oversight over the implementation of surveillance measures was also taken into account by the CJEU in the Schrems II judgment as that "*[...] the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'."*[181]

3.2.3.2 Internal Oversight

3.2.3.2.1 Inspectors General

189. The EDPB recognises that the Inspectors General are entrusted with a wide range of authorisations, necessary to monitor the intelligence activities. In particular, the Inspectors General have access to all information necessary to assess overall compliance of the work of the agencies with the legislation, including but not limited to the laws related to privacy and data protection and can issue subpoenas as well as take an oath from any person in relation to investigation of the Inspectors General.

190. Based on the above, the EDPB considers that the Inspectors General generally have extensive investigatory powers. However, they do not have any binding remedial powers and only issue non-binding recommendations[182].

191. The EDPB recognizes that in principle the Inspectors General shall not be prevented or prohibited from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigations.[183] In this context, the EDPB notes, however, that the

[176] ECtHR, Case of Klass and Others v. Germany, 6 September 1978 (hereinafter, 'ECtHR Klass judgment'), paragraphs 17, 51.
[177] ECtHR Zakharov judgment, paragraph 258; ECtHR, Iordachi and Others v. Moldova, 10 February 2009, paragraphs 40 and 51; ECtHR, Dumitru Popescu v. Romania, 26 April 2007, paragraphs 70-73.
[178] ECtHR Klass judgment, paragraph 56.
[179] ECtHR Zakharov judgment, paragraph 278.
[180] ECtHR Zakharov judgment, paragraph 283; ECtHR, L. v. Norway, 9 June 1990; ECtHR, Kennedy v. the United Kingdom, 18 May 2010, paragraph 166.
[181] CJEU Schrems II judgment, paragraph 179.
[182] Draft Decision, recital 105.
[183] Inspector General Act of 1978, § 3 (a).

Inspectors General are under the authority, direction and control of the respective head of department, who may prohibit them from access to information, undertaking an investigation and among others from issuing any subpoena in cases where the head of department determines that such a prohibition is necessary to preserve national interests. However, the head of department has to inform the responsible committees of the U.S. Congress of the exercise of this authority.[184]

192. The EDPB notes that Inspectors General can only be removed by the U.S. President, who must inform to Congress the reasons for such a removal.

193. The EDPB notes that there have not been significant amendments to the internal oversight mechanism since the opinions of the WP 29 and then the EDPB. Therefore, the EDPB follows, in line with the WP 29 Opinion 01/2016[185] that in general sufficient internal oversight mechanisms are in place.

3.2.3.3 External Oversight

194. The EDPB notes that besides the bodies mentioned below, various other bodies within the U.S. government oversee the activities of the U.S. intelligence agencies such as the Intelligence Oversight Board (IOB) or the Congressional committees. The latter can carry out their own investigations and reports.

3.2.3.3.1 Privacy and Civil Liberties Oversight Board (PCLOB)

195. The EDPB recognises the comprehensive supervision role of the PCLOB regarding the new redress mechanism and the implementation of the EO 14086.

196. Firstly, its new functions contain consultation with the Attorney General regarding the appointment of the judges of the DPRC and the special advocates. Secondly, the PCLOB will review the redress process annually, i.e. the processing of qualifying complaints by the redress mechanism. This includes whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner, are obtaining full access to necessary information and operating consistent with the EO 14086 as well as the Intelligence Community's compliance with the determinations made by the CLPO and the DPRC.

197. Furthermore, the PCLOB must be consulted while intelligence agencies update their internal policies and procedures to implement the EO 14086. In addition, the PCLOB will carry out a review of the updated policies and procedures and assess their compliance with the EO 14086.[186] While the findings of the PCLOB are not binding stricto sensu, the head of each element of the Intelligence Community is obliged to carefully consider and implement or otherwise address all recommendations contained in any such review, consistent with applicable law[187]. The EDPB invites the Commission to pay special attention to whether and how the PCLOB's recommendations have been implemented at agency level in future reviews, if the Draft Decision is adopted.

198. The EDPB recalls that the PCLOB, as it is independent, is "encouraged" to carry out but not obliged to review, if the safeguards constituted in EO 14086 are properly considered and whether the Intelligence Community fully complied with the requirements of the redress process. However, it is the

[184] See, e.g. Inspector General Act of 1978, § 8 (for the Department of Defence); § 8E (for the DOJ), § 8G (d)(2)(A),(B) (for the NSA); 50. U.S.C. § 403q (b) (for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (for the Intelligence Community).
[185] WP29 Opinion 01/2016.
[186] EO 14086, Section 2(c)(iv) and Section 2(c)(v).
[187] EO 14086, Section 2(c)(v)(B).

understanding of the EDPB that the PCLOB has stated in its additional explanation to the EDPB as well as in public[188] that it will take on the role foreseen in EO 14086.

199. Furthermore, the EDPB welcomes that the results of the PCLOBs reports are intended to be released to the public. Taking into account that the various bodies within the redress mechanism and the ones of the Intelligence Community have in principle to implement the recommendations in the reports of the PCLOB or otherwise address them, the EDPB recognises that these recommendations play an important role of privacy safeguards.

200. The EDPB notes that the PCLOB's access to information is restricted, if the U.S. President authorizes the conduct of "covert actions"[189] by departments, agencies or entities of the United States Government.[190]

201. Following its previous opinions, the EDPB considers the PCLOB as an independent body, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various surveillance programs, to be an essential element of the oversight structure.

202. However, the EDPB regretted in its 3rd Annual Joint Review of the former EU-U.S. Privacy Shield that the PCLOB provided the EDPB only with the same information as the general public. Furthermore, it was regrettable that the PCLOB did not issue further reports on PPD-28 to follow up on its first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a general updated report on Section 702 FISA.

203. Therefore, the EDPB welcomes the announcement of the PCLOB towards the EDPB, that the publication of a follow up report on Section 702 FISA can be expected in the near future. Furthermore, the EDPB is satisfied that the PCLOB informed about its commitment to allow publicity of its reports regarding the EO 14086. However, the EDPB recalls that the release of unclassified reports is regulated by U.S. law and must be coordinated with the Agencies of the Intelligence Community and cannot be decided by the PCLOB on its own accord.

204. Therefore, if the Draft Decision is adopted, the EDPB recalls that in future reviews of the EU-US data protection framework, the EDPB security cleared experts should be able to review additional documents and discuss additional classified elements as necessary to ensure that the information in the reports can be adequately assessed, while taking into account relevant national security interests and applicable privacy protections.

205. The EDPB welcomes the PCLOB's independence and oversight of the national intelligence community, which has to comply with the recommendations of the PCLOB or otherwise address it, which will be indicated in the report of the PCLOB to the U.S. Congress.

[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf
[189] According to 50 U.S.C. §3093(e)(1) the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities […].
[190] 42 U.S.C. § 2000ee (g) (5); 50 U.S. Code § 3093(a)

206. Taking into account the requirements of the ECtHR regarding public scrutiny[191] that the reports of a supervisory body have to be laid before and discussed by Parliament, the EDPB considers it sufficient, that the PCLOB submits its reports not less than semiannually to the U.S. President and in particular to the Congressional committees of the Senate and House of Representatives[192], which are the parliamentarian bodies of the U.S.

3.2.3.3.2 Foreign Intelligence Surveillance Court (FISC)

207. The Foreign Intelligence Surveillance Court is responsible for the oversight of the collection of personal data pursuant to Section 702 FISA[193] and the decisions of the FISC can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR).

208. The FISC oversees the certification process for the collection of foreign intelligence information pursuant to Section 702 FISA and authorizes electronic surveillance, physical search and other investigative measures for foreign intelligence purposes.[194] The FISC also authorizes the procedures for targeting, minimizing and querying the certificates, which are legally binding on U.S. intelligence agencies.[195] If the FISC finds that the requirements have not been met, it may deny the certification in full or in part and require the procedures to be amended.

209. If violations of targeting procedures are identified, the FISC can order the relevant intelligence agency to take remedial action.[196] These remedies range from individual to structural measures, e.g. from terminating data acquisition and deleting of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff.

210. The EDPB acknowledges that EO 14086 provides that the CLPO and the DPRC are to report violations to the Assistant Attorney General for National Security, who shall report those violations to the FISC.[197]

211. As the CJEU noted in its Schrems II decision, the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs[198]. Therefore, the EDPB maintains its concern that the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons which appears not to be resolved by the new EO 14086.

212. With regard to prior independent authorisation[199] of surveillance under Section 702 FISA, the EDPB regrets that, as the EDPB understands from the Draft Decision[200] and explanations provided by the U.S. Government, the FISC does not appear to be bound by the additional safeguards of the EO 14086, when certifying the programs authorising the targeting of non-U.S. persons. In the view of the EDPB, the additional safeguards contained in this order should nevertheless be taken into account in this context. The EDPB recalls that reports of the PCLOB would be particularly useful to assess how the

[191] ECtHR Zakharov judgment, paragraph 283, ECtHR, L. v. Norway, 9 June 1990; ECtHR, Kennedy v. the United Kingdom, 18 May 2010, paragraph 166.
[192] 42 U.S.C. §2000ee, (e).
[193] 50 U.S.C. 1881 (a)
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] 50 U.S.C.1881a (i)
[196] 50 U.S.C. § 1803 (h)
[197] EO 14086, Section 3 (c) (i) (D); EO 14086 Section 3 (d) (i) (F)
[198] CJEU Schrems II judgment, paragraph 179.
[199] For the collection of data in bulk under EO 12333 where the FISC is not competent, the EDPB is concerned, that there is not a prior authorization process in place for the collection of data in bulk (see also Guarantee B).
[200] Draft Decision, recital 165.

safeguards of the EO 14086 will be implemented and how these safeguards are applied when data is collected under Section 702 FISA.

3.2.4 Guarantee D - Effective remedies need to be available to the individual

213. The EDPB recalls that effective and enforceable rights of the individual are of fundamental importance for the finding of an adequate level of data protection in a third country. Data subjects must have an effective remedy to satisfy their rights when they consider that they are not or have not been respected. The CJEU explained in its Schrems I and II decisions that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[201]

214. The U.S. system relating to judicial remedies contains an important limit that makes it very difficult to bring legal proceedings against surveillance measures by the U.S. Government before ordinary courts. The U.S. constitution requires an individual to demonstrate standing, i.e. to establish a "concrete, particularized, and actual or imminent injury".[202] In surveillance cases such requirement appears to be nullified by the lack of notification to individuals subjected to surveillance even after these measures have ended.

215. In this context, the EDPB welcomes that EO 14086 establishes a specific redress mechanism to handle and resolve complaints from non-U.S. individuals, concerning U.S. signals intelligence activities. Under this new mechanism, the standing requirement is not applicable: according to Section 4(k)(ii) of EO 14086, the claimant does not need to show that their data has in fact been subject to U.S. signals intelligence. Data subjects can thus invoke the safeguards provided for in EO 14086, including those foreseen by other relevant laws and provisions as referred to in Section 4(d)(iii) of EO 14086.[203] In this regard, the new mechanism adds a redress avenue which would otherwise not exist.

216. The new mechanism comprises two layers: Under the first layer, individuals are able to lodge a complaint with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO). At the second level, individuals have the possibility to appeal the decision of the CLPO before a newly created body, the so-called Data Protection Review Court (DPRC). The following sections primarily focus on the second tier of the redress mechanism. The EDPB considers that the CLPO, as acting government official, is not vested with a sufficient degree of independence from the executive and thus cannot, of itself, adequately fulfill the requirements following from Article 47 of the Charter. This assessment has been confirmed by the Commission on several occasions.

3.2.4.1 Can the establishment of the DPRC based on an Executive Order per se be sufficient

217. The DPRC is not an ordinary court established by Congress under Article III of the U.S. constitution but is based on an Executive Order issued by the U.S. President. While the EDPB is aware of and generally welcomes the underlying consideration, namely avoiding the requirement to demonstrate standing (see also paragraph 215), this raises a fundamental question: Can such redress mechanism meet the requirements of Article 47 of the Charter (at all)? According to this provision everyone whose rights

[201] CJEU Schrems I judgment, paragraph 95; CJEU Schrems II judgment, paragraph 187.
[202] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p.10.
[203] EO 14086, Section 5(h) explicitly creates an entitlement for data subjects to submit complaints in accordance with the redress mechanism.

and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal previously established by law.

218. While the English wording of Article 47 of the Charter refers to a "tribunal", other language versions give preference to the word "court".[204] In Schrems II the CJEU has reiterated that "data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data".[205] However, in the same context of assessing the adequacy of the level of data protection, the CJEU considers that an effective judicial protection against such interferences can be ensured not only by a court, but also by a body, which offers guarantees essentially equivalent to those required by Article 47 of the Charter.[206] Likewise, the ECHR stipulates that "everyone whose rights and freedoms are violated shall have an effective remedy before a national authority"[207], which, as the ECtHR has consistently held, does not necessarily have to be a judicial authority.[208] Rather, the powers and procedural guarantees an authority possesses, in particular whether it is independent of the executive and ensures the fairness of the proceedings, are relevant to assessing the effectiveness of the remedy before that authority.[209] It appears that both courts do not base their assessment on purely formalistic criteria, but regard the substantive safeguards as decisive.

219. In Schrems II the CJEU has paid particular attention to effective redress in the area of national security access to personal data. The EDPB takes note that in doing so, the CJEU however did not discuss the "previously established by law" element of Article 47 of the Charter even though the Privacy Shield Ombudsperson mechanism was as well not based on U.S. statutory law. Instead of addressing this issue, the CJEU assessed different aspects for its adequacy test, such as the lack of remedial powers. Thus, the Schrems II judgment does not provide any guidance on the assessment of "previously established by law" according to Article 47 of the Charter. However, there are other rulings in which the CJEU has commented on this matter. Echoing the settled case-law of the ECtHR in that regard, the CJEU recalled in its cases C-487/19 and C-132/20 that the reason for the introduction of the term "previously established by law" is to ensure that the organisation of the judicial system in a democratic society does not depend on the discretion of the executive, but that it is regulated by law emanating from the legislature in compliance with the rules governing its jurisdiction.[210] As can be seen from this statement, the right to a tribunal previously established by law is very closely related to the guarantee of independence.

220. Against this background, the EDPB concludes that, in the context of assessing the adequacy of the level of protection, the specific redress mechanism created under EO 14086 as opposed to redress in Article III courts is not per se insufficient. The analysis of the level of protection in this respect depends on whether the safeguards provided in EO 14086 and complemented by the AG Regulation sufficiently ensure the independence of the DPRC vis-à-vis the other powers.

221. The Commission should continuously monitor whether the rules set forth in EO 14086 and its supplemental provisions, in particular those designed to foster the DPRC's independence, are fully

[204] For example "Gericht" in the German language version.
[205] CJEU Schrems II judgment, paragraph 194.
[206] See CJEU Schrems II judgment, paragraph 197.
[207] Article 13 ECHR.
[208] ECtHR Klass judgment, paragraph 67; ECtHR Big Brother Watch judgment, paragraph 359.
[209] ECtHR Klass judgment, paragraph 67; ECtHR Big Brother Watch judgment, paragraph 359.
[210] See CJEU, C-487/19, judgment of 6 October 2021, W.Ż, ECLI:EU:C:2021:798 and C-132/20, judgment of 29 March 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, paragraph 129 and paragraph 121.

implemented and are functioning effectively in practice. In addition, any amendments of the framework should be carefully reviewed for the impact on the Commissions assessment according to the Draft Decision. In this regard, the EDPB notes that changes to EO 14086 and the AG Regulation may trigger the adoption of immediately applicable implementing acts suspending, repealing or amending the adequacy decision.[211]

3.2.4.2 Sufficient independence from the executive

222. In its Schrems II ruling, the CJEU underlined that the independence of the court or body has to be ensured, especially from the executive, with all necessary guarantees, including with regard to its conditions of dismissal or revocation of the appointment. More specifically, the CJEU has criticized the fact that the Ombudsperson was appointed by and directly reporting to the Secretary of State. The Ombudsperson was held to be an integral part of the U.S. State Department. The CJEU also found there were no particular guarantees for the dismissal or revocation of the appointment of the Ombudsperson, hence undermining the Ombudsperson's independence from the executive.

223. The EDPB acknowledges that the provisions of EO 14086 and the supplemental AG Regulation do not impose a reporting obligation on the DPRC to the Attorney General, as would be the case in a superior-subordinate relationship. Nor is the DPRC subject to the Attorney General's "day-to-day supervision"[212]. These safeguards are a significant improvement over the Privacy Shield. However, the DPRC is established within the executive branch, namely the Department of Justice. For this reason in particular, the implementation and effective functioning of the safeguards in practice will be critical to determining whether the DPRC, although not an integral part of the Department of Justice, as an entity nevertheless located within the executive, can be considered sufficiently independent in practice. The EDPB calls on the Commission to monitor carefully whether these safeguards are fully reflected in practice. In addition, the EDPB suggests to clarify the term "day-to-day supervision" to the end that the "judges" of the DPRC are not subject to supervision of any kind. The Commission has confirmed that "day-to-day supervision" is meant to be understood in this sense.

224. Further to the above safeguards, the EU-U.S. DPF foresees certain guarantees regarding the appointment and dismissal of the DPRC "judges". While they are appointed by the Attorney General, their appointment is based on the criteria used to evaluate applicants for federal judgeships and involves a consultation of the PCLOB. Dismissal of "judges" prior to the expiration of their term of office or from an ongoing proceeding is possible only in narrowly defined circumstances, which, as the EDPB understands, are modeled on the provisions applicable to federal judges.[213] The application of these rules represents a further step to strengthen the independent position of the DPRC for which, again, implementation in practice will be crucial. However, it is not clear from the Draft Decision as such whether and how compliance with these requirements will be observed in the United States. Based on additional explanations provided by the Commission and the U.S. Government, the EDPB understands that the PCLOB may address the above mentioned provisions in its annual review of the redress process and that the responsibility to monitor and ensure compliance with all legal requirements of the Inspector General within the Department of Justice includes the requirements in EO 14086 and the regulations establishing the DPRC. The EDPB invites the Commission to clarify this aspect in the Draft Decision. That being said, the Commission should take these safeguards into account when monitoring the actual practice of the processing of personal data as assessed in the Draft Decision.

[211] Draft Decision, recital 212.
[212] AG Regulation, § 201.7 (d).
[213] EO 14086, Section 3(d)(iv); AG Regulation § 201.7.

225. The Draft Decision does not address the question whether, and if so, under which conditions the U.S. President has the authority to dismiss or remove "judges" from the DPRC. It is the understanding of the EDPB that such authority would not exist, as has been explained by the European Commission and confirmed by representatives of the U.S. government. The EDPB suggests to clarify this aspect in the adequacy decision.

226. The "judges" of the DPRC are appointed for four-year renewable terms and, at the time of their initial appointment, must not have been employed in the executive branch in the previous two years.[214] During their term of appointment as "judges" on the DPRC, they shall not have any other official duties or employment within the U.S. government.[215] They may however, unlike U.S. federal judges, participate in extrajudicial activities, including business activities, financial activities, non-profit fundraising activities, fiduciary activities, and the practice of law, where such activities do not interfere with the impartial performance of their duties or the effectiveness or independence of the DPRC.[216] Judicial independence derives not only from the freedom from instructions, but also from personal independence. In this context, factors such as the term of office, the possibility to be reappointed and the potential for conflicts of interest are relevant. The term of four years foreseen under EO 14086 and respectively the AG Regulation, while being e.g. shorter than the terms of office of judges of the CJEU (six years with the possibility of reappointment) and ECtHR (nine years without the possibility of reappointment), but as such does not give rise to serious concerns. The EDPB is not aware of any case-law imposing a minimum term of office in this respect[217]. The EDPB also recognises that the possibility to engage in extrajudicial activities is subject to the condition that, simply put, they do not lead to conflicts of interest compromising the duties on the DPRC. The EDPB understands from the U.S. Government`s additional explanations that these requirements are as well subject to the review and monitoring by the PCLOB and the Inspector General of the Department of Justice (see supra paragraph 226). How this requirement will be applied and demonstrated in practice should as well be addressed as part of the joint reviews.

227. Pursuant to Section 3(d)(i)(B) EO 14086 all "judges" of the DPRC must hold security clearances to be able to access classified information, i.e. to carry out their very function of adjudicating national security cases.[218] Some European laws and regulations on security clearance, in contrast, exempt judges from the requirement of a security clearance to the extent they perform judicial duties, regarding such detailed scrutiny as potentially conflicting with judicial independence.[219] According to explanations by the U.S. Government, while a candidate for a judicial appointment in a U.S. court undergoes a thorough vetting, after being appointed to serve as a federal judge in a U.S. court, a federal judge is not required to obtain a security clearance to access classified documents relevant to the case.

228. In the EDPB's view, the circumstances outlined above partly reveal differences between the position and status of a U.S. federal judge and a "judge" on the DPRC. However, the safeguards provided do not give reason to doubt the DPRC's independence. The EDPB urges the Commission that, should the Draft Decision be adopted, the above-mentioned safeguards be a priority during the first joint review

[214] AG Regulation § 201.3 (a).
[215] AG Regulation § 201.3 (c).
[216] AG Regulation § 201.7 (c).
[217] See also, mutatis mutandis, ECtHR (Grand Chamber), Case of Centrum För Rättvisa V. Sweden, 25 May 2021, paragraph 346.
[218] See also AG Regulation § 201.11 (b) and Draft Decision, recital 177.
[219] E.g. § 2(3) German Security Clearance Law.

of the EU-U.S. DPF. Furthermore, the EDPB expects the Commission to follow up on their commitment to suspend, repeal or amend the decision, if adopted, in case the U.S. Executive choses to restrict the safeguards included in the EO[220].

3.2.4.3 Powers of the DPRC

3.2.4.3.1 Access to information

229. Effective legal protection requires that a court has sufficient investigatory powers to review the contested measure. In the Kadi II case the CJEU ruled in regard to Article 47 of the Charter that the Courts of the European Union are to ensure that a decision is taken on a sufficiently solid factual basis.[221] The CJEU states that "it is for the Courts of the European Union, in order to carry out that examination, to request the competent European Union authority, when necessary, to produce information or evidence, confidential or not, relevant to such an examination"[222], whereby "the secrecy or confidentiality of […] information or evidence is no valid objection"[223].

230. Pursuant to Recital 181 of the Draft Decision the DPRC reviews the determinations made by the CLPO based, at a minimum, on the record of the CLPO's investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an intelligence agency. The Draft Decision further states that the DPRC has access to all information necessary, which it may obtain through the CLPO. This is based on the provision of § 201.9(b) AG Regulation, which authorizes the DPRC to "request that the ODNI CLPO supplement the record with specific explanatory or clarifying information and that the ODNI CLPO make additional factual findings where necessary to enable the DPRC panel to conduct its review". It is the understanding of the EDPB that the assessment carried out by the DPRC is thus not in any way limited to the findings made by the CLPO at the first level of the new redress mechanism. On the contrary, the DPRC can seek both additional legal information and, importantly, further factual circumstances for its analysis of whether a covered violation has occurred. At the same time, the EDPB also notes that these generally extensive investigatory powers do not extend to direct access to the data held on the individual. The Commission has explained that the CLPO will always function as an intermediary when the DPRC requires further information. Therefore, the DPRC's access to information necessary to independently adjudicate an application for review relies, to a certain extent, on the CLPO providing the necessary information. The EDPB recognises that the CLPO has an obligation to "provide any necessary support" to the DPRC and intelligence agencies are obliged to provide the CLPO with access to information necessary to conduct the DPRC's review [224]. The EDPB also notes, however, that the CLPO itself is not independent and conducts the initial investigation of a complaint at the first stage of the redress procedure. Therefore, the EDPB welcomes that the PCLOB will verify during its annual reviews of the redress mechanism whether the DPRC has obtained full access to all necessary information[225]. In addition, the EDPB invites the Commission to include this aspect in the joint reviews, if the Draft Decision is adopted, to examine the implications of this system in practice.

[220] Draft Decision, recital 212.
[221] CJEU, Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, European Commission and Others v Yassin Abdullah Kadi, judgment of 18 July 2013 (hereinafter, 'CJEU Kadi II judgment'), paragraph 119.
[222] CJEU Kadi II judgment, paragraph 120.
[223] CJEU Kadi II judgment, paragraph 125.
[224] EO 14086, Section 3(c)(i)(H) and Section 3(d)(iii).
[225] EO 14086, Section 3(e)(i).

3.2.4.3.2 Remedial powers

231. One of the central deficiencies of the Privacy Shield that led to its invalidation by the CJEU in Schrems II was the lack of binding remedial powers for the Ombudsperson. The CJEU found that "there is nothing […] to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services".[226] The mere (political) commitment from the U.S. Government that the Intelligence Community would correct any violation of the applicable rules detected by the Ombudsperson did not suffice to ensure a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter.

232. Under the new redress mechanism, by contrast, the decisions taken by the CLPO and by the DPRC have binding effect.[227] The EDPB recognizes, on the one hand, that this authority is not limited to specific measures, but allows "appropriate remediation" to "fully redress" an identified covered violation. Notably, Section 4(a) of EO 14086 explicitly mentions the deletion of unlawfully collected data. On the other hand, the EDPB notes that the wording of Section 4(a) of EU 14086 creates some uncertainty as to the process of determining such "appropriate remediation". While a measure should be designed to fully redress a violation, consideration should also be given to "the ways that a violation of the kind identified have customarily been addressed".[228] The meaning and effect of such requirement is unclear. Therefore, the EDPB invites the Commission to closely monitor the remediation measures adopted in practice.

3.2.4.4 Filing a complaint under the new redress mechanism

233. The redress mechanism established under EO 14086 is only applicable to qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation.[229] Hence, in order to avail oneself of this legal protection, several conditions need to be fulfilled.

3.2.4.4.1 Designation as qualifying state

234. First of all, the country or regional economic integration organization, from where the data was transferred to the United States must have been designated as a qualifying state prior to the data transfer underlying the complaint.[230] It is evidently essential that the redress mechanism provided is available when the adequacy decision enters into application. Accordingly, Recital 196 of the Draft Decision provides that the entry into force of the decision is conditional, inter alia, on the designation of the Union as a qualified entity for the purposes of the redress mechanism. In fact, the Commission appears to assume that the designation will occur prior to the adoption of the decision, as the draft already includes a placeholder for the Attorney General's designation of the EU[231] (as opposed to including the designation as a condition precedent in the operative part of the Draft Decision).

3.2.4.4.2 Adverse affect on privacy and civil liberties interests and "standing"

235. A "qualifying complaint" needs to be based on an alleged "covered violation", which in turn requires a violation that adversely affects the complainant's individual privacy and civil liberties interests[232]. It is

[226] CJEU Schrems II judgment, paragraph 196.
[227] EO 14086, Section 3(c)(ii) and Section 3(d)(ii), respectively.
[228] EO 14086, Section 4(a).
[229] EO 14086, Section 3(a).
[230] EO 14086, Sections 4(d)(i), 4(k)(i).
[231] Draft Decision, footnote 320.
[232] EO 14086, Section 4(k)(i) and 4(d)(ii).

the understanding of the EDPB, based on additional explanations from the Commission, that "adversely affect" does not imply any form of restriction on the admissibility of a complaint. Rather, as the Commission stated, such adverse affect would pertain to any complaint concerning the processing of personal data for signals intelligence activities in violation of the provisions referred to in Section 4(d)(iii), e.g. the safeguards of EO 14086. The EDPB regrets that this is not specified in the text of the Draft Decision and invites the Commission to further clarify the notion of being "adversely affected" in order to ensure that any violation of the data subjects' rights are assessed and remediated and that there is no level of "gravity" to be demonstrated to have access to redress and appropriate remediation.

236. As already mentioned, a complaint under EO 14086 does not require the claimant to demonstrate standing (see paragraph 215)[233]. The EDPB welcomes the clarification in Section 4(k) EO 14086 that a "belief test" will be applied and that it is not necessary to show that the complainant's data has in fact been accessed through signal intelligence activities. The establishment of the redress mechanism is an important step, as the standing requirement makes it very difficult to challenge surveillance measures before ordinary courts in the United States.

237. Based on the above, the EDPB does not consider recourse to ordinary courts, to which the Draft Decision also refers[234], to offer an adequate level of protection[235]. In this regard, the EDPB recalls its concerns already many times expressed in relation to the standing requirement before ordinary courts[236]. Moreover, based on additional statements by the U.S. government, it is the understanding of the EDPB that while EO 14086 does not preclude recourse to the courts of general jurisdiction, it is uncertain how such a court would apply this Order. This question could be explored further in the future reviews, if the Draft Decision is adopted.

3.2.4.4.3 The procedure of a complaint

238. The EDPB endorses in principle the procedure for routing a complaint through supervisory authorities of the Member States and continues to believe that the identification of the complainant should take place on EU territory. However, as under the Privacy Shield Ombudsperson mechanism, the Draft Decision provides that a data subject who wishes to lodge such a complaint must submit it to a supervisory authority in an EU Member State competent for the oversight of national security services and/or the processing of personal data by public authorities[237]. In this respect, the EDPB recalls its concerns already expressed in the WP 29's Opinion on the Privacy Shield, for instance potential difficulties for individuals to identify the competent authority given the variety of supervision mechanisms of national security services in Member States[238]. Taking into account the involvement of the national data protection authorities in the application of and oversight on the EU-U.S. DPF it is more appropriate to channel complaints through them.

3.2.4.5 The decision of the DPRC

239. After the review of the complainant's application is completed, the DPRC must not reveal whether or not the complainant was subject to U.S. signals intelligence activities. Instead, the complainant is

[233] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p.10.
[234] Draft Decision, recital 187 et seq.
[235] See also CJEU Schrems II judgment, paragraphs 191, 192.
[236] See WP29 Opinion 01/2016, p. 43.
[237] Draft Decision, recital 169.
[238] WP29 Opinion 01/2016, p. 48, 49.

notified that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation"[239]. This standard response serves the generally legitimate purpose of protecting sensitive information about U.S. intelligence activities. However, the EDPB is concerned that EO 14086 does not provide for any exemptions to the standard response of the DPRC.

240. In the Kadi II case, the CJEU had to address the conflicting interests of state secrecy on the one hand and fair, and as far as possible, adversarial proceedings on the other. The CJEU ruled that in circumstances where overriding considerations to do with national security preclude the disclosure of information or evidence to the person concerned, it is none the less the task of the courts to apply, in the course of judicial review, techniques which accommodate legitimate security considerations about the nature and sources of information and the need to sufficiently guarantee the respect for the individual's procedural rights, such as the right to be heard and the requirement for an adversarial process[240]. The CJEU further specified that it is for the courts, when carrying out an examination of all the matters of fact or law produced by the competent European Union authority, to determine whether the reasons relied on by that authority as grounds to preclude that disclosure are well founded[241]. If it turns out that the reasons relied on by the competent European Union authority do indeed preclude the disclosure to the person concerned of information or evidence, it is still necessary to strike an appropriate balance between the requirements attached to the right to effective judicial protection, and those flowing from national security[242]. In order to strike such a balance, it is legitimate to consider possibilities such as the disclosure of a summary outlining the information's content or that of the evidence in question[243]. Although the court's findings do not impose requirements for the decision issued by a court but rather relates to the decision of the competent authority and to the conduct of judicial proceedings, they provide indications about the balancing of the above mentioned interests in the context of the right to effective legal protection. For further guidance, reference can also be made to the Big Brother Watch case, in which the ECtHR, alluding to the fairness of the proceedings and in particular to the principle of an adversarial process, held that the decisions of a judicial or otherwise independent body should be reasoned[244].

241. The EDPB recognizes that the decisions of the DPRC are indeed reasoned. The DPRC is expressly required to issue a written decision setting out its determinations and the specification of any appropriate remediation[245]. In addition, the EDPB notes that the individual will be notified if the information pertaining to a review by the DPRC has been declassified[246]. The EDPB also recognises the role of the special advocates foreseen in the new redress mechanism that includes advocating regarding the complainant's interest in the matter[247]. However, in light of the implications of the jurisprudence of the CJEU and ECtHR set out above and taking into account that the decision of the DPRC cannot be appealed but is final[248], the EDPB has concerns about the general application of the standard response of the DPRC. The EDPB recalls that the PCLOB will independently review the functioning of the new redress mechanism and invites the Commission to pay particular attention to

[239] EO 14086, Section 3(d)(i)(H). Section EO 14086 stipulates this response for the CLPO as well.
[240] CJEU Kadi II judgment, paragraph 125.
[241] CJEU Kadi II judgment, paragraph 126.
[242] CJEU Kadi II judgment, paragraph 128.
[243] CJEU Kadi II judgment, paragraph 129.
[244] ECtHR Big Brother Watch judgment, paragraph 359.
[245] AG Regulation, § 201.9 (g).
[246] EO 14086, Section 3(d)(v).
[247] AG Regulation, § 201.8 (g).
[248] AG Regulation, § 201.9 (g).

this issue, including any assessment on this aspect by the PCLOB, during future reviews of the decision, if adopted.

4 IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION

242. Concerning the monitoring and review of the Draft Decision, the EDPB notes that according to the case law of the CJEU, 'in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted an adequacy decision pursuant to [Article 45 GDPR], to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard'[249].

243. In addition, the EDPB notes that the letter from the DoC provides that the DoC and other US agencies, as appropriate, will hold meetings on a periodic basis with the Commission, interested EU DPAs, and appropriate representatives from the EDPB[250].

244. The EDPB considers that the state law protection in relation to access by law enforcement authorities, the derogation for temporary bulk collection in view of targeted collection by US national security authorities, the application in practice of the newly introduced principles of necessity and proportionality, including in the context of the UPSTREAM program, the interplay between the EO 14086 and the different U.S. legal instruments allowing U.S. intelligence agencies to collect and further process personal data, the implementing internal policies and procedures, how these safeguards will also be taken into account in the context of the oversight led by the FISC, and how the redress mechanism will function effectively, and the question of onward transfers, automated-decisions, substantive and effective oversight and enforcement of the DPF Principles as well as effective redress will deserve specific attention in the course of the next periodic reviews.

245. The EDPB notes that the review of the adequacy finding will take place after one year from the date of the notification of the adequacy decision to the Member States and subsequently at least every four years[251]. With a view to further strengthening the continuous monitoring of the adequacy decision, the EDPB calls on the Commission to carry out the subsequent reviews at least every three years.

246. Concerning the practical involvement of the EDPB and its representatives in the preparation and proceeding of the future periodic reviews, the EDPB reiterates that any relevant documentation should be shared in writing with the EDPB, including correspondence, sufficiently in advance of the reviews. As was the case for the reviews carried out under the Privacy Shield, the EDPB recommends that, at the latest three months before the review should take place, the modalities for the review are established and agreed between the Commission, the US administration and the EDPB.

247. Furthermore, the EDPB notes and welcomes that Recital 212 of the Draft Decision provides examples of modifications undermining the level of protection that may justify the initiation of an 'emergency repeal procedure' that focuses on modifications that could occur concerning the Executive Order 14086 and the related AG Regulation.

[249] CJEU Schrems I judgment, paragraph 76. See also Draft Decision, Article 3(4).
[250] Draft Decision, Annex III.
[251] Draft Decision, Article 3(4).

For the European Data Protection Board

The Chair

(Andrea Jelinek)