EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework

Adopted on 4 November 2024

Adopted

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On 10 July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. Article 3 of the adequacy decision requires the Commission to regularly review the decision, with the first periodic review to take place after one year from the date of the notification of the adequacy decision to the Member States. In line with Recital 212 of the adequacy decision, five representatives of the EDPB participated in the review meeting that was held in Washington D.C. on 18 and 19 July of 2024. The EDPB focused on the assessment of both the **commercial aspects** of the EU-U.S. Data Privacy Framework ('DPF') and on the **access by U.S. public authorities to personal data transferred from the EU to DPF-certified organisations**.

The EDPB welcomes the efforts made by the U.S. authorities and the Commission to implement the DPF, and takes positive note of several developments that took place since the adoption of the adequacy decision.

Concerning the **commercial aspects** of the DPF, the EDPB notes that the U.S. Department of Commerce took all relevant steps to implement the certification process for U.S. companies, including developing a new website, updating procedures, engaging with companies, and conducting awareness-raising activities. Similarly, the multi-layered redress system under the DPF has been updated and implemented and provides for several, easily accessible avenues for complaints from EU individuals. However, the very low number of eligible complaints received in the first year of the DPF appears to confirm previous concerns of the EDPB that the possibility for individuals to lodge complaints must be accompanied by proactive checks from the competent U.S. authorities on compliance with the substantial elements of the DPF Principles. Thus, the EDPB would like to encourage the Department of Commerce and the Federal Trade Commission to increase ex officio investigations as regards substantial compliance of certified organizations with all DPF Principles in the near future.

The EDPB would also like to incentivise the Department of Commerce to work on and publish practical guidance on the Accountability for Onward Transfer Principle of the DPF. Such guidance would ideally clarify the requirements that DPF-certified companies who receive personal data from EU exporters need to comply with when transferring such data to other third countries. The EDPB also believes that there is a need to settle the longstanding divergence in interpretation between EU and US authorities of the notion of 'HR Data' under the DPF. Therefore, the EDPB equally encourages the Department of Commerce to swiftly develop guidance on this matter that acknowledges the broad definition of HR Data under the DPF and lays out practical examples where HR Data would be processed under the DPF, explaining for each scenario which DPF Principles would be relevant. The EDPB stands ready to provide feedback to the Department of Commerce's guidance.

Concerning **access by U.S. public authorities to personal data transferred from the EU to DPF-certified organisations**, the EDPB recalls that the adequacy decision is based in particular on the Commission's favourable assessment of Executive Order 14086, which is effectively meant to remedy the deficits identified in the judgment of the CJEU in Case C-311/18. To this end, Executive Order 14086 provides for additional safeguards, most notably by introducing the concepts of necessity and proportionality into the U.S. legal framework on signals intelligence and establishing a new redress mechanism. In the first periodic review one year after the adoption of the adequacy decision, the EDPB focused on the effective implementation of these safeguards as well as on new developments concerning government access to personal data for national security purposes.

On the implementation of the principles of necessity and proportionality, the EDPB recognizes that the U.S. Intelligence Community's internal policies and procedures have been updated and published. The

EDPB would have welcomed, however, an opportunity during the periodic review to discuss examples that clearly identify how the principles of necessity and proportionality are specifically interpreted and applied at agency level. The EDPB expects that future reviews would address this point. The EDPB is not in a position to fully assess the implementation of necessity and proportionality in practice and highlights the need to continue to carefully monitor this aspect, including in future reviews.

On effective redress, the EDPB had already recognized significant improvements, especially relating to the powers of the Data Protection Review Court. U.S. authorities have subsequently taken measures to implement the redress mechanism of the DPF. The EDPB welcomes these important steps which include not only the designation of the EU, Iceland, Liechtenstein and Norway as qualifying states for the redress mechanism but also the appointment of eight judges and two special advocates to the Data Protection Review Court. The EDPB considers that the elements of the redress mechanism provided for in Executive Order 14086 are in place. At the time of the review, no complaint had been filed under the new framework by EU individuals. Also, the annual review of the redress mechanism carried out by the Privacy and Civil Liberties Oversight Board is still pending. The EDPB wishes to renew its call to the Commission to monitor the practical functioning of the different safeguards of Executive Order 14086 designed to ensure an essentially equivalent level of protection. The redress mechanism should remain a priority during future periodic reviews.

With regard to the re-authorisation of Section 702 of the Foreign Intelligence Surveillance Act, the EDPB takes positive note of the legislative changes which increase privacy protections and recalls that Executive Order 14086 remains fully applicable when requesting access to data under Section 702 of the Foreign Intelligence Surveillance Act. However, the EDPB regrets that the reform did not incorporate the recommendation of the Privacy and Civil Liberties Oversight Board to codify certain safeguards of the Executive Order in Section 702 of the Foreign Intelligence Surveillance Act, thus not taking the opportunity to introduce additional safeguards as also previously recommended by the EDPB. The EDPB is concerned that the amendment to the definition of “electronic communication service provider” under Section 702 of the Foreign Intelligence Surveillance Act does not meet the requirement of clear, precise and accessible law. Notwithstanding the safeguards of Executive Order 14086, this change creates uncertainty about the actual reach of Section 702 surveillance. The EDPB considers that it is important for the Commission to follow up on future developments concerning Section 702 of the Foreign Intelligence Surveillance Act and also encourages the Privacy and Civil Liberties Oversight Board to monitor these developments.

The EDPB underlines that an adequate level of protection must be ensured also with regard to governmental acquisition of personal data by U.S. intelligence agencies from data brokers and other commercial entities that is not captured by Executive Order 14086. The Commission should further assess and monitor this particular form of government access and its practical use cases.

The EDPB would find it appropriate for the next review of the DPF to take place within less than four years, taking into account the numerous important aspects of the adequacy decision and the implementation of the DPF that the EDPB has recommended the Commission to closely monitor. This would allow the Commission and the EDPB to follow up in a structured manner on comprehensive information from U.S. authorities and other stakeholders about the practical application of the DPF sooner than the legally-established maximum time limit for the review.

The European Data Protection Board

Having regard to Article 3(4) and Recitals 211 to 213 of the Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter 'GDPR') on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework (hereinafter 'Decision'),

HAS ADOPTED THE FOLLOWING REPORT

1 INTRODUCTION

1. On 16 July 2020, the Court of Justice of the European Union ('CJEU') invalidated 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 (the 'Privacy Shield'). The CJEU found that the laws on government access to data transferred to the U.S. for national security purposes disproportionately limited the rights enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (the 'Charter').[1] Moreover, the CJEU stated that the Privacy Shield did not provide guarantees essentially equivalent to those required by Article 47 of the Charter.[2]

2. Soon after, the Commission and the U.S. government entered into discussions on a new framework that addressed the issues raised by the CJEU. In March 2022, President von der Leyen and President Biden announced that they had reached an agreement in principle on a new transatlantic data flows framework, following the negotiations started in the wake of the Schrems II decision. On 13 December 2022, the draft adequacy decision was published and transmitted to the EDPB for its opinion as per Article 70(1)(s) of the GDPR. Subsequently, on 28 February 2023, the EDPB issued its opinion[3] (the 'Opinion') on this draft adequacy decision.

3. On 10 July 2023, the Commission adopted the adequacy decision on the EU-U.S. Data Privacy Framework[4] (the 'Decision'). The framework that applies to commercial entities processing data transferred from the Union under the Decision is the EU-U.S. Data Privacy Framework ('DPF'). Article 3 of the Decision requires the Commission to regularly review the Decision, with the first periodic review to take place after one year from the date of the notification of the adequacy decision to the Member States[5]. As under the Privacy Shield, the Decision states that the "participation in this meeting should be open to representatives of the members of the European Data Protection Board"[6]. Accordingly, five representatives of the EDPB participated in the review meeting that was held in Washington D.C. on 18 and 19 July 2024.

[1] See judgment of the CJEU of 16 July 2020, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, C-311/18 ('Schrems II'), §§ 184-185.
[2] Idem, § 192.
[3] EDPB Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework, adopted on 28 February 2023.
[4] Commission Implementing Decision EU 2023/1795 of 10 July 2023 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-U.S. Data Privacy Framework, OJ L 231/118, 20.9.2023.
[5] Idem, Article 3(4).
[6] Idem, Recital 212.

4. Based on the Opinion, the EDPB assessed both the commercial aspects of the framework, i.e. the application and enforcement of requirements applying to companies self-certified under the DPF, and government access to data transferred to the U.S. for the purposes of law enforcement and national security. Considering that the review was carried out after the first year of operation of the DPF, the EDPB focused in particular on verifying whether all elements provided for in the framework have been put in place and whether they function effectively in practice.

5. The Commission published its report of the first periodic review on 9 October 2024[7].

6. The EDPB's main findings from this first periodic review, stemming from written submissions as well as from oral contributions, are presented in this report.

2 ON THE COMMERCIAL ASPECTS OF THE EU-U.S. DPF

2.1 Self-certification process; oversight and supervision of compliance with the Principles

7. In this first year of the DPF, the focus of the U.S. Department of Commerce ('DoC') has been on implementing the self-certification process, including developing a new website, updating procedures, engaging with companies, and other outreach/awareness-raising activities. The EDPB welcomes the efforts of the DoC in this regard, which contributed to clarifying certification requirements for companies and increased the trust of increasing numbers of companies certifying under the DPF[8].

8. The lack of ex officio oversight and structural enforcement actions, both by the DoC, the U.S. Federal Trade Commission ('FTC') and the U.S. Department of Transportation ('DoT'), as regards substantial compliance of certified organisations with all DPF Principles is, as it was under the previous Privacy Shield, a point of concern for the EDPB. The EDPB considers it important that the tools foreseen already by the Privacy Shield and now the DPF to monitor compliance, such as spot checks, compliance review questionnaires, and the possibility to request information from certified companies, are used by the DoC[9]. The EDPB welcomes the plans of the DoC to build tools that will perform automated compliance checks. However, the EDPB considers that automated means may complement but cannot substitute individual investigations and assessments of concrete cases. The EDPB stresses the importance of carrying out ex officio compliance monitoring activities and will devote significant attention to this aspect during the next review of the DPF.[10] The same goes for enforcement action by the FTC and the DoT. The EDPB notes that there are typically very few complaints by concerned individuals that might trigger enforcement action[11]. Therefore, the EDPB sees the need for proactive enforcement action for example by checking compliance with specific DPF Principles by certified companies of specific industry sectors.

[7] Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-U.S. Data Privacy Framework, COM(2024) 451 final, available at https://commission.europa.eu/document/download/25695177-8073-4ce3-bf81-eb816dc6b468_en?filename=Report%20on%20the%20first%20periodic%20review%20of%20the%20functioning%20of%20the%20adequacy%20decision%20on%20the%20EU-US%20Data%20Privacy%20Framework.pdf.

[8] COM(2024) 451 final, p. 2.

[9] For instance, DPF Principle 3(b) allows the DoC to request from certified companies a summary or representative copy of the relevant privacy provisions of their contracts for onward transfers.

[10] This has been previously underlined by the EDPB, notably in EDPB: EU - U.S. Privacy Shield - Third Annual Joint Review, adopted on 12 November 2019, para. 7 of the Executive Summary and para. 59.

[11] Idem, paras. 7 and 66.

9. While there were more than 2800 organizations listed as active participants under the DPF at the time of the review, there were also more than 1100 that had withdrawn from the DPF and 2600 listed as inactive because those participants had let their certification lapse. The DPF foresees that the DoC verifies whether organizations that actively withdraw from the DPF or let their certification lapse return, delete or retain the personal data received under the DPF. If the organization retains the data, it is obliged to continue to apply the DPF Principles and identify a contact point for further contacts. So far, the website of the DPF does not display if the inactive organizations have chosen to return, delete or retain personal data. Also, for those cases where the organizations have let their certification lapse, it is unclear if they have responded to the DoC and clarified whether the data received was returned, deleted, or retained. Given the significant number of inactive participants to the DPF this will also be an aspect that the EDPB will follow up on during the next review.

2.2 Complaint-handling, independent recourse mechanisms and arbitration

10. U.S. trade organisations and certified companies indicated before the review in responses to questionnaires sent out by the Commission that very few (if any) complaints from EU individuals had been received in the first year of the DPF. The EDPB notes that both DPF-certified companies and the dispute resolution bodies have invested considerable resources into ensuring transparent and accessible complaint procedures for EU individuals. However, the Independent Recourse Mechanism (IRM) providers present at the review meeting similarly reported to have received very few eligible complaints, of which several had been withdrawn or discontinued when the complainant failed to respond.[12] The few eligible complaints appeared to concern mainly requests for deletion of or access to personal data.

11. The first Annual IRM reports under the DPF were published shortly after the review meeting, confirming the overall very low number of eligible complaints received.[13] The reports were not presented in a standardised format and did not always include an explanation of how conflicts of interest were precluded. To ensure better comparability in the future, the EDPB would like to reiterate its recommendation that the DoC introduces a standardized template format for the Annual IRM report which includes explanation on how possible conflicts of interest are precluded.[14]

12. Neither the EU DPAs nor the DoC had received any complaints from EU individuals concerning non-compliance with the DPF Principles at the time of the review, although comprehensive guidance on the complaint procedure had been published on both sides of the Atlantic[15]. The EU DPAs and the DoC had also not received any referrals of DPF complaints from other authorities. The FTC reported having received two complaints that concerned, among other matters, questions of substantive compliance

[12] In the review meeting, two independent recourse mechanisms (IRMs) provided information about their DPF-related activities in the last year. While reporting an increase in companies requesting their services under the DPF in comparison to the situation under its predecessors, the two IRMs together had received only eight eligible complaints (out of 113 in total). Two of the eligible complaints concerned requests for access and deletion and were resolved, while four were withdrawn or discontinued due to a lack of response from the complainant. Two remained pending at the time of the review.

[13] The annual reports of all IRMs contained information about only one additional eligible complaint, bringing the total number to 9 in the first year of the DPF.

[14] See EDPB: EU - U.S. Privacy Shield - Third Annual Joint Review, adopted on 12 November 2019, para. 68.

[15] In April 2024, the EDPB adopted the Rules of Procedure for the "Informal Panel of EU DPAs" according to the EU-US Data Privacy Framework | European Data Protection Board (europa.eu). On the same date, the EDPB also published a template complaint form for submitting commercial related complaints to EU DPAs and an EU-U.S. DPF FAQ for European individuals, which were published on the websites of the national DPAs. The DoC also published guidance for European individuals on their rights under the DPF, including on the complaint procedure.

with the DPF Principles. However, they had not yet concluded any investigations or reached a decision in these cases.

13. The binding arbitration mechanism (International Centre for Dispute Resolution) stated that eleven arbitrators had been appointed for the EU-U.S. DPF Panel. In addition, the arbitration rules for the Panel and a code of conduct for arbitrators had been updated and adopted.[16] The arbitration mechanism had not been invoked at the time of the review.

14. The EDPB takes positive note of the significant efforts made to update and implement the many redress avenues available under the DPF and welcomes the awareness-raising and accessible guidance published on both sides of the Atlantic for the purpose of facilitating EU individuals' right to complain about certified organisations' non-compliance with the Principles. However, based on the feedback collected during the review, notably the very low number of eligible complaints submitted and the fact that these complaints concerned mainly requests for deletion of or access to personal data, the EDPB recalls that the easy access to redress for EU individuals under the DPF must be accompanied by proactive checks from the competent U.S. authorities on certified organisations' compliance with the substantial elements of the Principles[17].

2.3 Guidance and cooperation

15. Since the Decision entered into force, both the DoC, the EDPB and the Commission have published guidance, including in the form of FAQs, addressed to individuals, as well as to EU data exporters and U.S. importers[18]. The EDPB welcomes that the DoC is committed to clarifying aspects related to adherence to the DPF, compliance with the DPF Principles, and enforcement of the DPF, via the publication of guidance, and encourages the DoC to continue to do so, in particular for the benefit of U.S. data importers.

16. The EDPB would like to incentivise the DoC to work on and publish practical guidance for US importers on the **Accountability for Onward Transfer Principle** of the DPF. This topic was covered in the FAQs issued by the DoC on the Privacy Shield. At the time, such guidance was highly demanded by participating organisations, and the EDPB welcomed its adoption[19]. However, at the time of drafting this Report, the DoC had not included this topic in the guidance it has issued on the DPF. The EDPB takes note that DPF-certified companies would greatly benefit from practical guidance of the DoC on this topic, in particular concerning the concrete steps they have to take to comply with the Accountability for Onward Transfer Principle. The EDPB is especially concerned with the fact that some U.S. importers may not be aware of the requirements for lawful transfers of personal data received from EU exporters to third countries that have not been considered adequate by the Commission under Article 45 GDPR. The contributions to the DPF review received from some industry associations

[16] Information to European individuals on the arbitration mechanism is available here: ICDR-AAA DPF Annex I Services EU-US and UK | How to File | ICDR.org (adr.org).

[17] See, for previous remarks of the EDPB on this matter under the Privacy Shield, EDPB: EU - U.S. Privacy Shield - Third Annual Joint Review, adopted on 12 November 2019, para. 67.

[18] See, on the part of the DoC, https://www.dataprivacyframework.gov/US-Businesses; on the part of the EDPB, https://www.edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf, https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en and https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en; and on the part of the Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[19] EDPB Report on the EU - U.S. Privacy Shield - Second Annual Joint Review, Adopted on 22 January 2019, paras. 41 and 42.

show that certain DPF-certified companies may be relying on tools to carry out onward transfers that do not provide the same level of protection for the onward transferred personal data as the one guaranteed by the DPF Principles[20]. Any guidance of the DoC on the Accountability for Onward Transfer Principle should 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[21]. The EDPB remains available to provide inputs to draft guidelines of the DoC on this matter.

17. During the review, the EDPB stressed the need to settle the longstanding issue concerning the interpretation of the notion of '**HR Data**' under the DPF. The divergence of interpretation between EU and U.S. authorities (and its practical consequences) has been repeatedly mentioned by the EDPB in its reports concerning the annual reviews of the DPF's predecessor, the Privacy Shield. While the DoC has long taken view that only the processing of data of employees within the same corporate group falls within the category of 'HR data' under the DPF, the EDPB always regarded 'HR data' as any personal data concerning an employee in the context of an employment relationship, irrespective of whether the data is transferred within a corporate group or to a different commercial operator[22]. The EDPB believes that its interpretation is supported by the reference to 'unaffiliated service providers' in the definition of HR data in the DPF[23], and that EU exporters may only transfer HR Data under the DPF to U.S. importers that have an active HR Data certification and that conform to the requirements set forth in the Supplemental Principles set out in Section III (9) of the DPF. The EDPB acknowledges that some of the Supplemental Principles foreseen for HR Data under the DPF (such as specific requirements of Notice and Choice) may not have a practical application in scenarios where the U.S. importer does not have a direct or indirect relationship with the data subject nor access to his or her personal data 'in the clear'. However, the EDPB stresses the importance of ensuring the competence of EU DPAs in all scenarios where HR Data is transferred under the DPF, as provided under Section III (9)(d) of Annex I of the DPF.

18. The EDPB welcomes that the DoC has expressed its willingness to develop guidance to U.S. companies on the topic of HR Data in the months following the review to settle this interpretative divergence, which has important practical consequences. The DoC has mentioned that such guidance would seek to clarify the notion of HR data under the DPF, as well as contain different practical examples where employee data would be processed under the DPF (e.g. within a corporate group, by a service provider offering HR solutions, by an external cloud provider, etc.) and explain for each scenario which DPF obligations would be relevant. Among the goals of the guidance, the DoC has also underlined the need to prevent any potential enforcement gaps of DPF Principles. The EDPB is available to provide feedback to the DoC's draft guidance on the matter before publication, and hopes that this cooperation will lead to a common view among EU and U.S. authorities.

2.4 Relevant legal developments in the U.S.

19. Since the Decision came into force, there have been a number of developments in the legal framework in the U.S. in the area of privacy. This includes legislative and regulatory developments, as well as new

[20] See recital (38) of the Decision.
[21] EDPB 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, paragraphs 58 and 59.
[22] See Article 29 Data Protection Working Party, EU – U.S. Privacy Shield – First annual Joint Review (WP 255), Adopted on 28 November 2017, p. 9. 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 (SWD(2019) 390 final), p. 17 and 18.
[23] Section III (9)(a)(i) of Annex I of the DPF.

jurisprudence, which are outlined in detail in the European Commission's report on the first periodic review of the DPF[24].

20. In particular, the EDPB welcomes that twenty U.S. States have enacted comprehensive privacy laws as of July 2024, of which nine have entered into application, namely California, Colorado, Oregon, Virginia, Connecticut, Utah, Montana, Texas and Florida. On the other hand, the EDPB understands that the chances of a federal data protection law being enacted during the current terms of Congress and Senate, according to the representative of the U.S. National Telecommunications and Information Administration ('NTIA') present at the review meeting, seem to be low. The EDPB notes that a robust federal data protection law in the U.S. would play a positive role in ensuring the stability of an adequacy decision under Article 45 GDPR in relation to the U.S.

21. The EDPB has also stressed the importance of ensuring that the DPF or the U.S. legal system provide specific legal guarantees to individuals whose personal data are transferred from the EU under the Decision and who are then subject to decisions which produce legal effects concerning or significantly affecting them and which are based solely on the automated processing of their personal data. While no such legal guarantees stem from the DPF itself and there are only specific safeguards provided by relevant U.S. Federal law in specific areas[25], the EDPB takes positive note that the FTC has recently increased the use of its enforcement powers against discrimination and bias in automated systems in cases of substantial injury to consumers[26]. The EDPB also welcomes that 17 U.S. States have adopted legislation addressing the automated processing of personal data (or, at least, some forms of it) and generally allowing opt-outs for certain types of decision-making based on "profiling"[27].

22. Lastly, the EDPB takes note of the recent judgment of the U.S. Supreme Court in *Loper Bright Enterprises v. Raimondo* (of 28 June 2024), which overrules previous case law on the so-called *Chevron doctrine*. Under this doctrine, courts were bound to apply the principle of deference to a regulatory agency's reasonable interpretation of the law in case of ambiguity in a law enforced by that agency. During the review, EDPB representatives echoed concerns expressed by NGOs that the recent judgment could affect the powers of the FTC to enforce privacy cases and to issue regulations in the area of privacy[28]. In response, the FTC explained that the ruling does not affect its enforcement powers and that it generally exercises rulemaking powers under the Magnuson-Moss Warranty Act[29], and not under the Administrative Procedures Act (which is the one affected by the *Loper Bright Enterprises v. Raimondo* judgment). U.S. authorities competent for the oversight of law enforcement and national security agencies also confirmed that the *Loper Bright Enterprises v. Raimondo* judgment does not affect their competences to supervise compliance with the safeguards applicable to personal data processing in those contexts.

[24] COM(2024) 451 final, p. 8-10.
[25] Recital (35) of the Decision.
[26] See as an example, https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v. It is noteworthy that, in this decision, the FTC requires the company to provide several phases of notice to affected consumers and to grant them the ability to challenge automated decisions.
[27] COM(2024) 451 final, p. 9.
[28] https://fpf.org/blog/chevron-decision-will-impact-privacy-and-ai-regulations/.
[29] https://www.ftc.gov/legal-library/browse/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act.

3 ON THE ACCESS AND USE OF PERSONAL DATA TRANSFERRED UNDER THE DECISION BY U.S. PUBLIC AUTHORITIES

23. The Commission's finding of an essentially equivalent level of data protection for the collection and use by U.S. public authorities of personal data transferred to controllers and processors in the U.S. is based in particular on the Commission's assessment of Executive Order 14086 on enhancing safeguards for U.S. signals intelligence activities ('EO 14086' or 'EO'). EO 14086 is effectively meant to address and remedy the deficits identified by the CJEU in its Schrems II ruling, which invalidated the previous adequacy decision, called the Privacy Shield. To this end, EO 14086 provides for additional data protection safeguards, most notably by introducing the concepts of necessity and proportionality into the U.S. legal framework on signals intelligence and establishing a new redress mechanism for individuals in the area of signals intelligence activities.

24. In the Opinion, the EDPB recognized significant improvements compared to the former Privacy Shield framework while also noting points for further attention or for concern. Taking these points into account, the EDPB's focus in the first periodic review one year after the adoption of the Decision was on the effective implementation of the safeguards foreseen in EO 14086 as well as on new developments concerning government access to personal data for national security purposes. As regards the legal framework applicable to access to data for law enforcement purposes, there have been no relevant developments, as confirmed by the U.S. authorities that took part in the review. In this report, as in its previous analyses and the Opinion, the EDPB follows 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.

25. Against this background, the report addresses a number of specific issues that were discussed in detail during the periodic review with U.S. authorities.

3.1 Implementation of necessity and proportionality

26. As a key finding of the Opinion, the EDPB emphasized that EO 14086 introduces the principles of necessity and proportionality in the U.S. legal framework on signals intelligence. At the same time, the EDPB underlined the need to monitor closely the effects of this change in practice.[30] In light of this, a central objective of the periodic review was to further examine how the U.S. Intelligence Community (IC) applies necessity and proportionality in a day-to-day context.

3.1.1 Internal policies and procedures

3.1.1.1 Implementation of necessity and proportionality

27. Section 2(c)(iv) of EO 14086 obliges IC agencies to update their internal policies and procedures as necessary to implement the EO's safeguards within one year of the date of EO 14086. In addition, and as one of the specific oversight functions entrusted to the Privacy and Civil Liberties Oversight Board ('PCLOB') under EO 14086, Section 2(c)(v) mandates the PCLOB to conduct a review of the updated policies and procedures to ensure that they are consistent with the safeguards contained in the EO. On that basis, the EDPB understands that the updated policies and procedures are intended to operationalize the safeguards set forth in EO 14086 at agency level. They are therefore critical to assessing whether these safeguards, in particular the principles of necessity and proportionality,

[30] See EDPB 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, p. 5.

effectively function in practice. The PCLOB's representatives - namely, the PCLOB's Chair and three Board Members -, stated during the periodic review that the PCLOB expects to undertake its review of the internal policies and procedures in the near term.

28. The EDPB recognizes that the agencies' policies and procedures have been updated and also published on the website of the Office of the Director of National Intelligence ('ODNI'), thus complying with the aforementioned obligation under Section 2(c)(iv) of the EO. The relevant website reads: "*The IC elements' procedures released today further implement the EO's requirements, and thereby the United States' commitments under the EU-U.S. DPF. As required by the EO, each IC element developed its procedures in consultation with the Attorney General, the ODNI Civil Liberties Protection Officer (CLPO), and the Privacy and Civil Liberties Board. In implementing the EO's safeguards, each set of procedures is tailored to the authorities, missions, and responsibilities of the IC elements*".[31] This was confirmed by the ODNI CLPO during the periodic review. In this context, the EDPB also welcomes that, according to additional explanations provided, intelligence agencies carry out dedicated staff trainings on the requirements of EO 14086.

29. While acknowledging the statements made by U.S. authorities as well as the binding nature of the EO's safeguards, the EDPB would have welcomed an opportunity during the periodic review to discuss concrete examples that clearly identify how the introduction of the principles of necessity and proportionality affect the actual practice of the IC's data collection and processing of personal data; in other words, how these principles are specifically interpreted and applied by U.S. intelligence agencies. The EDPB expects that future reviews would address this point. It would have been particularly helpful to clarify whether and, if so, what changes have resulted for agencies' day-to-day operations from the introduction of necessity and proportionality requirements compared to the legal situation prior to the adoption of EO 14086.

30. The EDPB is not in a position to fully assess the implementation of necessity and proportionality in practice and highlights the need to continue to carefully monitor this aspect, including in future reviews of the DPF. In this respect, the EDPB considers that the PCLOB review will be particularly helpful for further understanding and examining this matter. Consequently, the EDPB invites the Commission to pay special attention to whether the PCLOB identifies any shortcomings in the internal policies and procedures as well as how any recommendations issued by the PCLOB are addressed.

3.1.1.2 Amendments and departures

31. Many, if not all, of the internal policies and procedures that have been made available to the public contain provisions permitting amendments and departures from those policies and procedures under certain circumstances, e.g., depending on the immediacy or gravity of a threat to national security[32]. These provisions generally provide that all activities in all circumstances must be conducted in a manner consistent with the Constitution and laws of the United States.[33] In response to a request from EDPB representatives, the ODNI CLPO confirmed during the periodic review that any amendments or departures must thus always comply with EO 14086. The internal policies and procedures do not and cannot authorize IC elements to deviate from the EO and the safeguards contained therein.

32. Despite this assurance, the EDPB would like to better understand the nature of such amendments and departures and their possible practical implications. The EDPB would need more information, including

[31] See https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086, where the policies and procedures are also available.
[32] See, for example, Section 1(4) National Security Agency (NSA) Procedures.
[33] See, for example, Section G(3) Central Intelligence Agency (CIA) Procedures.

practical examples of such amendments and departures, in order to assess their actual impact on the protection of personal data. It is unclear to the EDPB how, in practice, a deviation from the general rules in policies and procedures of IC agencies would still fulfil the requirements of EO 14086. As indicated above, the EDPB welcomes the PCLOB's impending review of the implementing internal policies and procedures, which could provide further clarity on this point.

3.1.2 Updates of legitimate objectives

33. EO 14086 defines twelve objectives for which signals intelligence collection activities can take place (Section 2(b)(i) EO 14086).[34] The U.S. President may update this list of legitimate purposes with additional – not necessarily public – objectives in light of new national security imperatives (Section 2(b)(i)(B) EO 14086). During the first periodic review, the U.S. Government stated that this authority has not been used to date.

34. The EO details a specific procedure to determine and validate, on the basis of the above mentioned legitimate objectives, more concrete signals intelligence collection priorities.[35] This procedure includes an assessment by the ODNI CLPO whether such priority (1) advances one or more legitimate objectives; (2) was neither designed nor anticipated to result in signals intelligence collection for a prohibited objective and (3) was established after appropriate consideration for the privacy and civil liberties of all persons (Section 2(b)(iii)(A) EO 14086).

35. Hence, the EDPB assumes that the ODNI CLPO, through their capacity in the validation process, would in principle also assess those intelligence priorities that would pursue a covertly added objective. However, as the legitimate purposes constitute an important limitation for surveillance activities and restrict, e.g., the broader notion of "foreign intelligence information" referred to in Section 702 of the Foreign Intelligence Surveillance Act ('FISA'), the EDPB stresses the importance of subjecting the possibility of establishing secret objectives to further and independent oversight mechanisms. From discussions with the PCLOB during the periodic review, the EDPB has learned that the PCLOB may be able to review secret updates of the list of legitimate objectives following a request for classified information. The EDPB welcomes this possibility and would like to encourage the PCLOB to consider this issue for future oversight projects.

3.1.3 Prior independent authorisation of bulk collection

36. In the Opinion, the EDPB identified, as a problematic aspect in the current regime on government access to data, that the U.S. legal framework, when allowing for the collection of data in bulk, neither provides for the requirement of prior authorisation by an independent authority, as required in the

[34] As well as five prohibited objectives for which signals intelligence collection must not be conducted (Section 2(b)(ii) EO 14086).

[35] As outlined in Section 2 of EO 14086, the legitimate objectives cannot by themselves be relied upon to justify signals intelligence activities, but need to be further substantiated into so-called intelligence priorities. For instance, the test for necessity and proportionality is not directly linked to a legitimate objective, but to a "validated intelligence priority". Section 2(a)(ii)(A) and (B) of EO 14086 thus read: "*signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority* […]" and "*signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized* […]".

jurisprudence of the European Court of Human Rights ('ECtHR'), nor for a systematic independent ex post review by a court or an equivalently independent body.[36]

37. The first periodic review did not provide any new information or developments that affect the EDPB's previous analysis in this respect. The EDPB therefore maintains its concern as raised at the time. Moreover, the EDPB considers that recent case law of the ECtHR further supports its standpoint, as the Court has once again emphasized the importance of independent prior authorisation of secret surveillance measures.[37]

3.2 Re-authorisation of Section 702 FISA

38. Section 702 FISA governs electronic surveillance targeting non-U.S. persons who are reasonably believed to be outside of the United States to obtain foreign intelligence information. Due to a "sunset" clause, Section 702 FISA was scheduled to cease having legal effect on 31 December 2023, unless re-authorised by Congress. On 19 April 2024, Congress passed the Reform Intelligence and Securing America Act ('RISAA')[38], which extends Section 702 FISA for two years from the date of its enactment, introducing several amendments. The EDPB takes positive note of the legislative changes increasing privacy protections, such as the statutory prohibition of "abouts" collection, expedited declassification of Foreign Intelligence Surveillance Court ('FISC') decisions as well as additional accountability, oversight and reporting requirements, which the Commission's report on the first periodic review highlights in more detail[39]. This report focuses on the changes to Section 702 FISA that the EDPB deems to be particularly important for the Decision and that were discussed extensively during the periodic review.

39. Before looking at these specific changes more closely in sections 3.2.1 and 3.2.2, the EDPB wishes to draw attention to some more general issues. First, it should be noted that EO 14086 remains fully applicable when requesting access to data under Section 702 FISA, i.e. also after the amendments made by RISAA. This understanding of the interplay between the EO and the statutory provisions governing the collection of data by the IC was confirmed during the periodic review. As a further general remark, the EDPB regrets that RISAA did not incorporate the PCLOB's recommendation to codify certain safeguards of EO 14086 in Section 702 FISA, thus not taking the opportunity to introduce additional safeguards as also previously recommended by the EDPB[40]. In its report on the surveillance programme operated pursuant to Section 702 FISA, released on 28 September 2023, the PCLOB in particular proposed that Congress should codify the twelve legitimate objectives for signals intelligence collection as laid out in EO 14086[41]. The PCLOB elaborated that such codification would align the definition of foreign intelligence in the EO and Section 702 FISA and confer explicit jurisdiction to the FISC to enforce the EO when evaluating Section 702 FISA collection practices. It would thus allow the FISC to use the standards for foreign intelligence under the EO in FISA-related rulings and court

[36] See EDPB 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, p. 5 and 33, 34.
[37] See judgment of the ECtHR of 28 May 2024, Pietrzak and Bychawska-Siniarska and Others v. Poland, legal summary point (c), available at https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-14333%22]}.
[38] https://www.congress.gov/bill/118th-congress/house-bill/7888#:~:text=%2F09%2F2024)-,Reforming%20Intelligence%20and%20Securing%20America%20Act,on%20surveillance%20under%20Section%20702.
[39] COM(2024) 451 final, p. 12 et seq.
[40] See for instance Article 29 Working Party, EU-U.S. Privacy Shield – First annual Joint Review, p. 3.
[41] https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf.

procedures. Against this background, the EDPB invites the Commission to continue monitoring developments with respect to Section 702 FISA, including in the context of its renewal after two years.

3.2.1 Expansion of "electronic communication service provider"

40. Most notably, RISAA expanded the definition of "electronic communication service provider" ('ECSP'), i.e. the entities that may be required to disclose personal information under Section 702 FISA. In addition to the previous wording, the definition now also covers "*any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications*"[42]. Various stakeholders have strongly criticized this change, arguing that the new wording could compel most U.S. business to assist with Section 702 FISA surveillance[43].

41. U.S. authorities explained to the EDPB that this amendment stems from a legal dispute before the FISC and the Foreign Intelligence Surveillance Court of Review ('FISCR'). According to U.S. authorities, the objective of extending the notion of ECSP is, in response to said litigation, to include a certain class of companies that was ruled to fall outside the previous definition as interpreted by the FISC and FISCR.[44] The U.S. Department of Justice ('DoJ') stressed during the periodic review that the modification, despite its broader wording, was thus merely aimed at addressing the specific scenario encountered in the relevant FISC and FISCR decisions and would only be applied narrowly. While both decisions have been publicly released[45], they contain substantial redactions that include the type of company in question. Therefore, it is not possible from those judgments to understand what specific kind of company is actually concerned.

42. The U.S. Attorney General confirmed the explanation provided by the DoJ during the periodic review in a letter to Congress. In this letter, the DoJ commits to applying the new subset of the definition exclusively to cover the type of service provider at issue in the litigation before the FISA courts. It is further stated therein that the number of companies captured by the amendment to the ECSP definition is "*extremely small*"[46]. In light of persisting public concerns, a further legislative change has been introduced with the draft Intelligence Authorization Act for Fiscal Year 2025 that, if passed by Congress, would enact such narrow interpretation by limiting Section 702 FISA directives to "*a provider of the type of service at issue in the covered opinions*", i.e. the FISC and FISCR opinions initially prompting the new ECSP definition.[47] By making general reference to these decisions, which were only published with redactions (see above), neither the DoJ letter not the draft bill specifies the actual type of company. Thus, both RISAA and the draft bill leave secret an element of the legal parameters for Section 702 FISA surveillance.

43. In this regard, the EDPB wishes to recall the first of the four so-called "European essential guarantees", according to which, following from Articles 8(2) and 52(1) of the Charter, "processing should be based

[42] 50 U.S.C. § 1881 (b)(4)(E), with exceptions for public accommodation facilities, dwellings, community facilities and food service establishments.

[43] See e.g., https://cdt.org/wp-content/uploads/2024/05/letter-to-garland-and-haines-re_-ecsp-provision-1.pdf.

[44] As far as the EDPB understood, this was also due – and the subsequent change effectively meant to address – changes in electronic communications and internet technology since Section 702 FISA was initially passed.

[45] Available at https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf and https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf.

[46] DoJ letter dated 18 April 2024, available at https://www.justice.gov/opa/media/1348621/dl?inline.

[47] Section 1202 draft Intelligence Authorisation Act for Fiscal Year 2025, available at https://www.congress.gov/bill/118th-congress/senate-bill/4443/text#toc-H704B2609C40F4870A02125404F3FF3B7.

on clear, precise and accessible rules".[48] 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.[49] While "*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*"[50], clear rules on secret surveillance measures are essential to prevent the risks of arbitrariness and abuse where a power vested in the executive is exercised in secret. In that sense, the "*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*"[51].

44. The EDPB is concerned that the new subset of the ECSP definition as incorporated by RISAA does not, and the envisaged provision of the draft Intelligence Authorisation Act for Fiscal Year 2025 would not meet the requirement of clear, precise and accessible law – both for individuals whose personal data may be accessed and for companies now subject to Section 702 FISA. With regard to the latter, questions also arise in relation to legal remedies against FISA disclosure directives: in particular, the EDPB would welcome clarification concerning the information that will be available to those companies now falling within the revised definition and, accordingly, on what basis they would have to decide whether to challenge such a directive before the FISC. Notwithstanding the safeguards of EO 14086, which, as stated, continue to apply, the current definition of ECSP creates uncertainty about the actual reach of Section 702 FISA surveillance, also considering that the FISC lacks statutory jurisdiction to enforce the EO's safeguards.

45. In this context, the EDPB moreover observes that – although the newly inserted subset of the definition may only cover an "extremely small" number of companies – the amount of personal data potentially in scope of a collection under Section 702 FISA could be significantly increased. For instance, if such limited number of companies processes large volumes of personal data or accounts for a large percentage of the respective market.

46. As already indicated above, the EDPB considers that it is important for the Commission to follow up on future developments concerning Section 702 FISA, including in particular the application of the broadened ECSP definition in practice. In this regard, the EDPB notes that U.S. Attorney General will report to Congress within 6 months of the entry into force of RISAA on how the new definition of ECSP is being applied in practice. The EDPB would also like to encourage the PCLOB to monitor these developments, bearing in mind that its recent recommendation on the codification of the safeguards contained in the EO has not been implemented by RISAA. The EDPB regards the PCLOB's recommendations to be an important contribution to U.S. privacy reforms. As an independent body, the PCLOB is an essential element of the oversight structure.

3.2.2 Changes regarding the role of amici curiae

47. In addition, RISAA introduced changes regarding the role of the so-called amici curiae before the FISA courts. Amici curiae are non-governmental experts appointed to inform the court about specific legal

[48] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, p. 8.

[49] See judgment of the CJEU of 16 July 2020, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, C-311/18, §§ 174-175. See also judgment of the CJEU of 6 October 2020, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, C-623/17 Privacy International, § 65.

[50] ECtHR, Zakharov v. Russia, 4 December 2015, § 229.

[51] Idem.

or technical issues. As the FISC and FISCR consider FISA applications in secret in the interest of protecting national security, amici curiae serve an important role. They provide external perspectives before the FISC and FISCR that help address the one-sided nature of the ex parte proceedings (meaning the data subject is not a party to the proceedings before the court).

48. While RISAA positively foresees the routine appointment of an amicus curiae in cases in which a Section 702 FISA certification is at issue, RISAA also imposed certain limitations to their role. Whereas the former law required that amici curiae had expertise in privacy and civil liberties, intelligence collection, communications technology or other relevant areas, RISAA requires expertise in both privacy and civil liberties and intelligence collection. RISAA also bars amici from raising issues that the court has not asked it to address. Amici curiae are now "*limited to addressing the specific issues identified by the court*"[52].

49. The EDPB observes that, even if the rationale that might underlie the latter amendment is commendable, namely to improve the efficiency in FISA court proceedings, the principle of fairness and equality of arms behind the legal instrument of amici curiae carries significant weight. Even if, according to the information available to the EDPB, this change could be reversed by pending legislation, the EDPB invites the Commission to monitor future developments and ensure that the ability of the amici curiae to advise on the privacy interests of the public is not hampered.

50. Finally, but importantly, the EDPB notes that the aforementioned legislative changes have no impact on the status and role of the special advocates appointed in proceedings before the DPRC. U.S. authorities have clarified that the relevant provisions of EO 14086, complemented by AG regulation 28 CFR Part 201, are independent from the re-authorisation of Section 702 FISA.

3.3 Redress mechanism

51. On effective redress, the EDPB recognised in the Opinion significant improvements concerning the then newly established mechanism, especially relating to the powers of the DPRC and its enhanced independence compared to the Ombudsperson under the Privacy Shield. The EDPB also acknowledged the additional safeguards foreseen in the new redress mechanism such as the special advocates or the annual review by the PCLOB.

3.3.1 Developments relating to the redress mechanism

52. Since the Opinion, U.S. authorities have taken further measures to implement the redress mechanism. First, the EU, Iceland, Liechtenstein and Norway were designated on 30 June 2023 as qualifying states for purposes of eligibility for the redress mechanism, effective upon adoption of the Decision, i.e. as of 10 July 2023[53]. Subsequently, on 14 November 2023, the U.S. Attorney General appointed eight judges to the DPRC, subject to several requirements set forth in EO 14086 and supplementing regulations.[54] Specifically, the appointment of DPRC judges is based on the criteria used to evaluate applicants for federal judgeships and involves a consultation of the PCLOB. In addition, the judges must have appropriate experience in the fields of data privacy and national security law. On that note, the

[52] U.S.C. 50 § 1803 (i)(4)(A).
[53] https://www.justice.gov/d9/2023-07/Attorney%20General%20Designation%20Pursuant%20to%20Section%203%28f%29%20of%20Executive%20Order%2014086%20of%20the%20EU%20EEA.pdf.
[54] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

EDPB welcomes the exceptional professional expertise of the DPRC judges that is undoubtedly evident from the information published by the DoJ.[55]

53. Pursuant to paragraph 201.4 of AG regulation 28 CFR Part 201, the U.S. Attorney General has meanwhile also designated two special advocates. As set out Section 3(d)(i)(C) of EO 14086, special advocates shall assist the DPRC in its consideration of an application for review, including by advocating for the complainant's interest in the matter and ensuring that the DPRC panel is well informed of the issues and the law with respect to the matter.

54. Further, the EDPB takes positive note that the ODNI and the DoJ provide comprehensive information material on their websites, such as a presentation and an overview of the national security redress mechanism, frequently asked questions and, as mentioned earlier, detailed information on the individual DPRC judges and special advocates.[56] These resources contribute to explaining and raising awareness for the new mechanism. The EDPB has as well taken additional measures to operationalize the redress mechanism on the EU side, in particular by adopting a template complaint form to facilitate the submission and handling of complaints, and to raise awareness of the mechanism.[57] Furthermore, encrypted communication channels have been established for the transmission of complaints from supervisory authorities in the EU to the EDPB secretariat, and from the EDPB secretariat to the competent authorities in the U.S.

55. All these developments are decisive steps towards making the redress mechanism operational. The EDPB considers that the elements of the redress mechanism provided for in EO 18046 are in place. At the time of the review, however, no complaint had been filed under the new framework[58]. The redress mechanism had therefore not yet been triggered and put to the test in practice. Also, the annual review of the redress mechanism carried out by the PCLOB pursuant to Section 3(e) of EO 14086 is still pending. The PCLOB confirmed that the Board plans to start the review process soon. In the absence of complaints at the time of the review, the review focussed on the set-up of the mechanism in accordance with the legal requirements. It is against this background that the EDPB wishes to renew its call to the Commission to monitor the practical functioning of the different safeguards designed to ensure an essentially equivalent level of protection based on Article 47 of the Charter. The redress mechanism should remain a priority during future periodic reviews.

3.3.2 Independence of the DPRC

56. In its Opinion, the EDPB addressed in detail the question of the independence of the DPRC, concluding the safeguards provided by EO 14086 and the relevant U.S. Attorney General Regulation do not give reason to doubt the DPRC's independence. In announcing the DPRC judges, the U.S. Attorney General reaffirmed the DPRC's independence by stating: "*Although this court has been established at the Department of Justice, its judges will independently decide what remedies, if any, are appropriate for*

[55] https://www.justice.gov/opcl/redress-data-protection-review-court.
[56] https://www.justice.gov/opcl/dprc-resources; https://www.justice.gov/opcl/redress-data-protection-review-court; https://www.dni.gov/index.php/who-we-are/organizations/clpt/clpt-related-menus/clpt-related-links/signals-intelligence-redress-mechanism-icd-126; https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.
[57] The EDPB has adopted a template complaint form, an information note for the general public as well as rules of procedure governing cooperation between the national supervisory authorities and the Secretariat of the European Data Protection Board, which are available at https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en. The template complaint form is intended to be translated and published by all data protection authorities in their national languages.
[58] The EDPB Secretariat received a first complaint on 30 October 2024.

the cases in front of them, and the intelligence agencies will be expected to abide by their decisions."[59] As outlined above, it can be argued that the safeguards have yet to pass the practical test. It therefore remains important to monitor the effective functioning of these safeguards in practice, taking into account the particular nature of the DPRC as an entity located within the executive branch. The EDPB would find it particularly helpful if the PCLOB report following the first annual review of the redress mechanism would focus on the issue of independence of the DPRC in practice.

3.3.3 Standard response

57. With a view to the redress mechanism, the EDPB has in the past expressed its concern both 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 the fact that the DPRC's decisions cannot be appealed, taken together.[60] As the periodic review did not provide any new information or developments on this point, the EDPB considers this issue to remain relevant and maintains its concern. The EDPB thus also re-affirms its call to the Commission to closely monitor the practical functioning of the redress mechanism given its importance for the protection of the rights and interests of data subjects.

3.4 Government access to commercially available data

58. During the periodic review, several NGOs have drawn the Commission's and the EDPB's attention to the acquisition of personal data by U.S. intelligence agencies from data brokers and other commercial entities. Recently, there has also been increased media coverage of personal data for sale and resulting risks for both individual privacy rights and national security interests. It is clear that the volume and sensitivity of commercially available data have expanded over the past years due to the advancement of digital technology, including location tracking of smartphones and other devices as well as data collection for advertising purposes when using online services. It is also clear that such information can provide critical intelligence value. The EDPB believes this form of government access to personal data raises a number of privacy concerns. For the purposes of this report on the first periodic review of the DPF, the EDPB wishes to make the following observations.

59. As confirmed by U.S. authorities during the periodic review, the purchase of personal data by U.S. intelligence agencies does not fall under EO 14086, as the EO's scope is limited to signals intelligence activities. Consequently, the safeguards provided in the EO, including the redress mechanism, are not applicable to other forms of government access to personal data. U.S. authorities explained that there is nevertheless a legal framework establishing standards for how intelligence agencies acquire and use commercially available information, including Executive Order 12333 and a binding Intelligence Community Policy Framework[61] recently issued by the ODNI (the Policy Framework).

60. The Policy Framework states that "*the increasing availability of* [commercially available information] *and its potential sensitivity call for additional clarity in how the IC will make effective use of such*

[59] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

[60] See 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, p. 5 and 52. According to Section 3(d)(i)(H) of EO 14086, the Data Protection Review Court shall inform the complainant that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation".

[61] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf.

information while ensuring that privacy and civil liberties remain appropriately protected"[62]. To those ends, it establishes general principles and lays out a framework for the IC's access to and processing of certain sensitive forms of commercially available information, "*while allowing individual IC elements flexibility to experiment in the manner best suited to both meet the element's operational needs and protect privacy and civil liberties*"[63].

61. The general principles applicable to all commercially available information notably highlight that privacy and civil liberties shall be integral considerations in the acquisition and use of commercially available information. IC elements shall furthermore apply appropriate safeguards that are tailored to the sensitivity of the information. The principles also require that commercially available information is not used to disadvantage individuals based on traits such as race, gender, or religion. The framework further provides that agencies must assess the original source and quality of the data, manage and periodically review their implementation of safeguards, and provide appropriate transparency to the public and relevant oversight entities on their policies and procedures. Without assessing the Policy Framework in detail, the EDPB observes that it sets out several strong standards reflecting privacy interests. However, unlike EO 14086, it does not provide for the principles of necessity and proportionality, nor does it address legal remedies. It is also not clear whether and to what extent the safeguards contained in the Policy Framework apply to non-U.S. persons. With regard to Executive Order 12333, the EDPB recalls the findings of the CJEU in its Schrems II decision, according to which Executive Order 12333 does not provide an essentially equivalent level of protection. Overall, the acquisition of commercially available data appears to be less strictly regulated than government access to data through signals intelligence activities.

62. The EDPB considers this does not constitute a shortcoming of EO 14086, precisely because this form of data collection and processing is outside its scope. However, the acquisition by intelligence agencies of commercially available data could have the effect of EO 14086 and its safeguards being circumvented and thus practically watered down or undermined. From this perspective, the commercial acquisition of personal data by the IC and its practical use cases should be further assessed and monitored by the Commission. The EDPB emphasizes that an adequate level of protection must be ensured comprehensively, i.e. including with regard to the possibility of this particular form of government access. In this respect, the Commission's report on the periodic review refers to the Accountability for Onward Transfer Principle of the DPF, which self-certified organizations must comply with[64]. While it is true that the Accountability for Onward Transfer Principle is applicable in the case at hand, the EDPB considers that how this Principle is observed in practice in this specific context requires attention by the Commission. In particular, in the present scenario, it may be challenging to contractually require the third party to provide the same level of protection as the one guaranteed by the DPF.

63. The EDPB considers a report by the PCLOB on this issue particularly important, as it could provide recommendations on how the acquisition of commercially available personal data by intelligence agencies could be further addressed from a regulatory perspective. The EDPB positively notes that these matters are on the agenda of the PCLOB, as its representatives informed the EDPB during the periodic review. Namely, the PCLOB is currently analysing the U.S. Federal Bureau of Investigation's use of data purchases[65].

[62] Idem, p. 1.
[63] Idem, p. 2.
[64] COM(2024) 451 final, p. 16.
[65] https://www.pclob.gov/OversightProjects.

4 CONCLUSIONS & RECOMMENDATIONS

64. The EDPB welcomes the efforts made by the U.S. authorities and the Commission to implement the DPF, especially in relation to the redress avenues for EU individuals under the DPF Principles, as well as the appointments of the DPRC judges and special advocates. However, the EDPB still has identified during the first periodic review a number of points for additional clarifications, for attention or for concern.

65. Concerning the commercial aspects of the DPF, given that the certification process under the DPF generally seems to be running smoothly, the EDPB would expect the DoC to increase in the near future its ex officio oversight and structural enforcement actions as regards the substantial compliance of certified organizations with all DPF Principles. The Principles have remained largely unchanged compared to the Privacy Shield, and the need for more oversight activity in this area was previously identified by the Commission and the EDPB during the Joint Reviews of the Privacy Shield. The first periodic review of the DPF also points to a lack of monitoring activities in what concerns substantive compliance with the Principles. The need for proactive compliance monitoring becomes particularly clear in light of the very low number of complaints received in the first year of the DPF. The EDPB stresses the need for the Commission to carefully monitor this aspect, including in future reviews of the DPF.

66. Moreover, the EDPB would like to incentivise the DoC to work on and publish practical guidance on the Accountability for Onward Transfer Principle of the DPF. The EDPB is concerned that some DPF-certified companies may not be aware of the requirements for lawful transfers of personal data they have received from EU exporters to third countries that have not been considered adequate by the Commission under Article 45 GDPR. The EDPB also believes that there is a need to settle the longstanding divergence in interpretation between EU and US authorities of the notion of 'HR Data' under the DPF, which has important practical consequences. Therefore, the EDPB equally encourages the DoC to swiftly develop guidance on this matter that acknowledges the broad definition of HR Data under the DPF and that lays out practical examples where HR Data would be processed under the DPF, explaining for each scenario which DPF obligations would be relevant. The EDPB stands ready to provide feedback to the DoC's guidance on these two important matters.

67. With regard to government access to data, the EDPB would have welcomed the opportunity to discuss examples of how the principles of necessity and proportionality, introduced to the U.S. legal framework for signals intelligence collection by EO 14086, are specifically interpreted and applied at agency level. The EDPB thus highlights the need to continue to carefully monitor this aspect, including in future reviews of the DPF. While the elements of the redress mechanism provided for in Executive Order 14086 are in place, the redress mechanism had not yet been put to the test in practice, as at the time of the review no complaint had been filed under the new framework. The EDPB wishes to renew its call to the Commission to monitor the practical functioning of the different safeguards designed to ensure an essentially equivalent level of protection, taking into account the pending PCLOB reviews on the implementation of the EO's necessity and proportionality requirements and on the functioning of the redress mechanism.

68. The EDPB regrets that RISAA did not incorporate the PCLOB's recommendation to codify certain safeguards of the Executive Order in Section 702 FISA, thus not taking the opportunity to introduce additional safeguards as also previously recommended by the EDPB. The EDPB is concerned that the amendment to the definition of Electronic Communication Service Provider does not meet the requirement of clear, precise and accessible law – both for individuals whose personal data may be

accessed and for companies now subject to Section 702 FISA. The EDPB considers that it is important for the Commission to follow up on future developments concerning Section 702 FISA, including in particular the application of the broadened definition of Electronic Communication Service Provider in practice. The EDPB would also like to encourage the PCLOB to monitor these developments.

69. Finally, the EDPB emphasizes that an adequate level of protection must be ensured also with regard to the governmental acquisition of personal data by U.S. intelligence agencies from data brokers and other commercial entities that is not captured by EO 14086. The Commission should further assess and monitor this particular form of government access and its practical use cases.

70. The EDPB takes note of the suggestion of the Commission to carry out the next periodic review of the Decision after three years[66], and welcomes that the European Commission is therefore not proposing to apply the statutory maximum period of four years. This is due to the fact that there are numerous important aspects of the Decision and the implementation of the DPF that the EDPB has recommended the Commission to closely monitor. A review within three years or less would allow the Commission and the EDPB to more swiftly obtain comprehensive information about the practical application of the DPF, notably in what concerns the monitoring by the DoC and the FTC of substantial compliance of certified organizations with all DPF Principles. During that period, authorities in the EU and US may also gather more experience with handling complaints from individuals under the DPF, both on the commercial and on the government access to data sides. Lastly, the EDPB notes that the next re-authorisation of Section 702 FISA is due in two years, and that it would be important for the European Commission and the EDPB to take stock of a possible re-authorisation shortly after it occurs. This is particularly relevant given the broadening of the entities covered by FISA 702 requests in the latest re-authorisation. The EDPB looks forward to the consultation from the European Commission in accordance with Article 3(4) of the Decision on the periodicity of future reviews of the Decision.

For the European Data Protection Board

The Chair

(Anu Talus)

[66] COM(2024) 451 final, p. 21.