EUROPEAN
COMMISSION

Brussels, 9.10.2024
COM(2024) 451 final

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-US Data Privacy Framework

1. THE FIRST PERIODIC REVIEW - BACKGROUND, PREPARATION AND PROCESS

In its decision of 10 July 2023 (the "adequacy decision"), the Commission found that the EU-U.S. Data Privacy Framework (DPF) provides an adequate level of protection for personal data transferred from the European Union to organisations in the United States of America[1]. The adequacy decision requires the Commission to carry out periodic reviews, the first of which should take place after 1 year from the date of notification of the adequacy decision to the Member States. This report concludes this first review.

As required by recital 211 of the adequacy decision, this first review, taking place after the first year of operation of the new framework, focused on verifying whether all elements provided for in the framework have been implemented and are functioning effectively. The review covered all aspects of the functioning of the framework, including in light of legal developments that took place since the adequacy decision was adopted.

In preparation for the review, the Commission gathered information from relevant stakeholders, in particular from non-governmental organisations (NGOs) with expertise in digital rights and privacy[2], DPF-certified organisations, through their trade associations[3], as well as from the U.S. authorities involved in implementing the framework. Moreover, the Commission has also gathered feedback from the general public by means of a specific call for evidence on the "Have your Say" portal[4].

A review meeting took place in Washington D.C. on 18 and 19 July 2024. It was opened by EU Commissioner for Justice and Consumers Didier Reynders and U.S. Secretary of Commerce Gina Raimondo.[5]

For the EU, the review was conducted by representatives of the European Commission's Directorate General for Justice and Consumers, together with five representatives designated by the European Data Protection Board (EDPB) and coming from different national data

[1] 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-US Data Privacy Framework.

[2] The Commission sent a questionnaire to nine NGOs (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology) focusing on relevant developments in the U.S. legal framework, oversight and enforcement mechanisms, and the functioning of redress mechanisms. Commission services and the EDPB representatives also met online with these NGOs on 9 July 2024.

[3] The Commission sent a questionnaire to nine trade associations (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine), focusing on the experience of DPF-certified companies, in particular the certification process, steps taken to comply with the DPF Principles, mechanisms to deal with requests and complaints from individuals, etc.

[4] The feedback received can be found at the following link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_en.

[5] The review meeting was organised by topic, with each dedicated agenda point introduced by a short presentation by the relevant U.S. authority, EU representative or organisation followed by a detailed question-and-answer session. The "commercial aspects" of the framework (i.e. the application and enforcement of requirements applying to companies certified under the DPF) were covered on the first day, while issues relating to government access to personal data were discussed on the second day.

protection authorities (DPAs) and the European Data Protection Supervisor[6]. On the U.S. side, representatives from the Department of Commerce (DoC), the Department of State, the Federal Trade Commission (FTC), the Department of Transportation (DoT), the Office of the Director of National Intelligence (ODNI), the Department of Justice (DoJ), the Inspector General for the Intelligence Community, as well as members of the Privacy and Civil Liberties Oversight Board (PCLOB) participated. In addition, representatives from organisations offering independent dispute resolution services and the American Arbitration Association provided information during the relevant review sessions. Furthermore, the review was informed by presentations from DPF-certified organisations on how companies comply with the requirements of the framework.

The Commission's findings have further been informed by publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from non-governmental organisations, transparency reports issued by DPF-certified companies, annual reports from independent oversight bodies, as well as media reports.

2. FINDINGS

2.1. Commercial aspects

2.1.1. The certification process

In order to be able to receive personal data transferred from the EU on the basis of the DPF, a U.S. company must certify, and then re-certify on an annual basis, with the DoC its adherence to specific data protection requirements (the "DPF Principles"). The certification requires that a company is subject to the investigatory and enforcement powers of the FTC or the DoT, publicly declares its commitment to comply with the DPF Principles, and publicly discloses its privacy policy and fully implements such requirements[7]. Before finalising a certification, the DoC verifies whether the company has met all certification requirements[8].

At the review meeting, the DoC explained that, in this first year of the DPF, the focus has been on putting in place the certification process, including developing dedicated IT tools, updating procedures, engaging with companies, and carrying out other outreach/awareness raising activities. As at the date of the review meeting, more than 2800 companies have become DPF-certified. This means that more companies have become DPF-certified than under the previous framework, the Privacy Shield, in its first year of operation[9]. According to information provided by the DoC, 70% of the participants are SMEs and a large number of DPF companies (47%) are in the information, communications and technology (ICT) sector. Moreover, 60% of companies are certified exclusively for non-HR data, 2.5% companies are certified exclusively for HR data and 37.5% are certified for both HR and non-HR data.

The DoC has adopted the necessary procedures to handle applications from companies. Companies must submit their applications for certification on the DoC's DPF website

[6] The Commission and EDPB representatives met on 12 June and 10 July 2024 to prepare for the review, discuss the input received and identify which aspects require additional information-gathering and clarification.
[7] Section I.2 of Annex I to the adequacy decision.
[8] Annex III to the adequacy decision.
[9] In the equivalent period, 2400 companies had certified under the Privacy Shield.

(https://www.dataprivacyframework.gov/). It contains information on how to join the DPF[10] and on the company's obligations under the Framework[11]. A specific team in the DoC, under the responsibility of a dedicated Director for the Data Privacy Framework, is in charge of all aspects relating to the management and administration of the DPF, including the certification process and compliance monitoring. Each application is assigned to a specific staff member that remains responsible for the relevant company throughout the certification process.

To be certified under the Framework, companies submit their application, including a draft privacy policy. The DoC checks if it conforms with the relevant requirements of the DPF. When organisations want to certify different entities within a corporate group (e.g. different subsidiaries), the DoC asks for and reviews either one comprehensive privacy policy that clearly indicates all entities to be covered, or separate policies for each entity. The DoC also verifies with the independent recourse mechanism (IRM)[12] indicated in the application whether the organisation has actually registered with it. For companies that select the data protection authority panel (e.g. because they process HR data), the DoC checks whether the company has paid the required fees to make use of the panel. Where necessary, the DoC also verifies whether the applicant falls under FTC or DoT jurisdiction (and is therefore eligible to join the DPF).

If all conditions are met, the DoC informs the organisation that it can post its privacy policy referring to the DPF on its website. Once the privacy policy is public, the DoC confirms the certification and incorporates the company in the DPF list on its website. The DPF can be relied on to receive personal data from the EU from the date that the DoC places the organisation on that list[13].

As explained during the review meeting, the checks carried out by the DoC so far have resulted in 33 applications being rejected, because they did not meet the DPF requirements. In general, the DoC works with the company to address any deficiencies. Where the DoC identifies any deficiencies, it informs the company that it must address these and that failure to respond within a given timeframe, or other failure to complete their self-certification in accordance with the DoC's procedures, will lead to its application being considered abandoned. If the initial certification is not completed/amended within 12 months, the DoC considers it abandoned.

The due date for annual re-certification is specified in the DPF list for each company. To remind companies of the need to apply for re-certification, the DoC has created a system with reminders that the certification is about to expire. Organisations receive a reminder one month before, then two weeks before and then one day before the due date. Those that let their certification lapse are removed from the DPF list. As described under Annex III to the adequacy decision, the DoC has a specific section on its website listing the U.S. organisations that are not any longer active participants and identifying the respective reasons why (e.g. lapse or withdrawal) the concerned companies have been removed from the list (the "inactive list"). When organisations are removed from the DPF list for having allowed their certification to lapse the DoC contacts them to confirm whether they wish to withdraw or instead intend to re-certify, and, if the latter, to verify that during the lapse they have applied the DPF Principles to personal data received under the DPF and to clarify what steps they will take to address the

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements

[12] Private sector dispute resolution mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual.

[13] Section I, Paragraph 3 of Annex I to the adequacy decision.

outstanding issues that have delayed their re-certification. When companies notify the DoC that they wish to withdraw from the DPF, the DoC requires them to confirm whether they will return or delete the data received under the DPF; retain it and continue to apply the DPF Principles to such data (which has to be confirmed annually); or retain it and put in place other protections (such as standard contractual clauses adopted by the European Commission).

Feedback received from trade associations and companies indicates that DPF-certified companies have taken a number of steps to ensure compliance with the DPF Principles. For example, to comply with the *recourse, enforcement and liability principle*, organisations have carried out internal checks either conducted by means of self-assessment or via external compliance review. The two private-sector IRMs that participated in the review meeting explained that they also provide external compliance review by reviewing privacy policies, and one of the private-sector IRMs explained that it also provides audits and random checks, focusing for instance on the *access*, *choice* and *onward transfer* principles. In addition, certified companies have developed internal compliance programs and oversight mechanisms, trained employees, implemented mechanisms to allow individuals to exercise their rights, carried out privacy impact assessments, and reviewed existing contracts.

2.1.2. Compliance monitoring, false claims of participation and enforcement

Under the DPF, the DoC is responsible for monitoring compliance with the DPF Principles through the use of different tools, including *ex-officio* checks (on its own initiative), *ad hoc* spot checks and compliance questionnaires. This includes searching for and addressing false claims of participation in the framework, for instance through internet searches[14].

To monitor compliance with the Principles by DPF companies, the DoC has mainly relied on ad hoc web searches and (social) media checks over the past year. The DoC reported that it has not detected issues of compliance with the DPF Principles in this first year and has not referred any companies to the FTC or DoT for possible enforcement action. It has also set up a dedicated point of contact to facilitate cooperation with DPAs and receive complaints from individuals and referrals from other authorities (e.g. DPAs or the FTC). However, no referrals or complaints have been received over the past year. Whereas this first year of operation of the DPF was focused on setting up the framework and the certification process, at the review meeting, the DoC explained that it plans to carry out compliance checks by automated means in order to perform them in a more systematic way, and is currently developing the necessary IT tools to do so.

The Commission acknowledges that the DoC needed to focus its efforts in this first year on setting up the Framework and the certification process. Moving forward, it is important that the DoC steps up its efforts to monitor and check compliance with the Principles, which is necessary to ensure a continued high level of compliance with the framework and detect cases requiring further enforcement action, including possible false claims of participation by companies. In this regard, the Commission welcomes the fact that the DoC confirmed its intention to develop and use (automated) tools to more effectively and systematically identify compliance issues and false claims and is of the view that this should be part of a broader effort to make greater use of the different tools at its disposal (e.g. spot checks, compliance review

[14] See Annex III to the adequacy decision. False claims may arise, for instance, when a company claims to participate in the DPF and it either never started the certification process, or has started it but has not brought it to an end or has allowed its certification to lapse.

questionnaires, information requests etc.), including to verify compliance with specific requirements under the DPF[15].

DPF organisations are subject to FTC and DoT jurisdiction. During the review meeting, the DoT confirmed that it has all processes in place to take appropriate enforcement action. It also explained that very few companies under its jurisdiction have joined the DPF (i.e., a few ticket agents but no airlines). The FTC confirmed that it systematically checks for DPF violations in each of its privacy investigations. So far, the FTC has not received any referrals from other authorities. It has received a few complaints mentioning the DPF, although two of them concerned companies on the "inactive list", two concerned companies that were not participating in the framework and one did not concern personal data transferred from the EU. At the time of this report, the FTC had not issued decisions to enforce compliance with the DPF, although it confirmed that several companies that are DPF-certified are currently under investigation.

The Commission welcomes the fact that the FTC systematically checks for DPF violations in all its privacy investigations. As the continued effectiveness of the DPF depends on its robust enforcement, it is expected that the FTC will further exercise its investigative powers under the framework, including by proactively carrying out sweep actions focusing on compliance with specific DPF requirements and/or certain sectors.

2.1.3. Complaint handling

The DPF provides EU individuals with different recourse possibilities for cases of non-compliance with the DPF Principles by certified organisations[16]. This includes, pursuing resolution through direct contacts with a DPF organisation, which must provide a response to the affected individual within 45 days. Individuals may also bring a complaint to an IRM designated by an organisation to investigate and resolve complaints. Depending on the circumstances, this could be either an alternative dispute resolution body or a DPA[17]. Finally, in case none of the other available redress avenues has satisfactorily resolved the data subject's complaint, individuals may trigger binding arbitration before the EU-U.S. DPF Panel as a recourse of last resort.

2.1.3.1. Complaint handling by companies

The responses from trade associations and companies to questionnaires sent by the Commission indicate that DPF-certified companies have received very few – if any – complaints from individuals concerning non-compliance with the DPF Principles. At the same time, companies have put in place different mechanisms and tools to allow individuals to exercise their rights and lodge complaints, including via web-based forms, email, and phone.

2.1.3.2. *Independent Recourse Mechanisms (IRMs)*

The feedback received during the review meeting and the information provided by trade associations indicates that there have been a very low number of complaints to independent resolution mechanisms. IRMs that have been selected by companies include BBB National

[15] For instance, concerning onward transfers, by making use of the possibility under DPF Principle 3(b) to request a summary or representative copy of the relevant privacy provisions of contracts for onward transfers.
[16] See Section 2.4 of the adequacy decision.
[17] DPF organisations are obliged to cooperate in the investigation and the resolution of a complaint by a DPA either when it concerns the processing of HR data collected in the context of an employment relationship or when the respective organisation has voluntarily submitted to oversight by DPAs.

Programs, JAMS, TRUSTe and VeraSafe. The DPF requires that the IRMs publish an annual report with aggregate statistics on the use of their dispute resolution services. At the time of the adoption of the present report, all concerned IRMs had published their annual reports[18].

Moreover, at the review meeting, BBB and VeraSafe made detailed presentations on their activities from the last year. They reported an increase in the number of business participants choosing their services in comparison with previous frameworks and mentioned that they had received some complaints, although the vast majority were ineligible. For example, BBB received 87 complaints from EU individuals, with only two of them eligible for resolution. Although BBB explained that complaints are on average processed in 5 business days on average, those two complaints were eventually closed because of a lack of response from the individuals. VeraSafe received 26 complaints, of which six were eligible for resolution. Two of those concerning requests for access and deletion were resolved, while two remain pending, and two were either withdrawn or closed because of a lack of response from the individual. Both IRMs explained that they aim to answer complaints in the individual's language.

DPF companies that process HR data transferred from the EU must select the EU DPAs as their IRM for that data, whereas a DPF company may on a voluntary basis select the EU DPAs as their IRM for other types of personal data transferred in reliance on the DPF. In fact, more than half of the companies certified under the DPF at the time of the review opted for this solution[19], which is welcomed. Since the adequacy decision was adopted, the EDPB has adopted the rules of procedure for the "Informal Panel of EU DPAs". The Panel is competent for providing binding advice to the U.S. organisations following unresolved DPF complaints from individuals about the handling of personal data that has been transferred from the EU under the DPF. According to its rules of procedure, the panel is formed by one DPA acting as lead DPA and other designated co-reviewer DPAs[20]. It provides binding advice within 60 days of receiving a DPF complaint. The EDPB has also published a template complaint form for

[18] ANA - https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs - https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA - https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0 ;
Insights association - https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS - https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf ;
Privacy Trust DPF Services - https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf ;
TRUSTe Dispute Resolution - https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf ;
Verasafe - https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf

[19] Shortly after the date of the review meeting, the DPF website indicated that 1511 of the 2892 participants had an EU Data Protection Authority as its Recourse Mechanism.

[20] On 17 April 2024 the EDPB adopted the Rules of Procedure for the "Informal Panel of EU DPAs" according to the EU-US Data Privacy Framework. It can be accessed here: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

submitting complaints to DPAs,[21] as well as "FAQs for European individuals"[22] and businesses[23] on the DPF. The Panel had received no complaints at the time of the review.

2.1.3.3. The binding arbitration mechanism

The International Centre for Dispute Resolution (ICDR) which is the international division of the American Arbitration Association, was selected by the DoC to administer the binding arbitration mechanism. Following the adoption of the adequacy decision, the DoC, together with the Commission, selected 11 arbitrators with experience in privacy and from various backgrounds, including arbitration, the judiciary, academia and civil society[24]. Moreover, the arbitration rules[25] for the DPF Panel and a code of conduct for arbitrators[26] have been adopted, and are all available on the ICDR website. At the time of the review, the arbitration mechanism had not been triggered yet by any individual in the EU.

2.1.4. Guidance, cooperation and awareness-raising

Since the DPF entered into force, the DoC has carried out various awareness-raising activities by organising roadshows, webinars and conferences; reaching out to trade associations and interacting directly with more than 3000 companies to provide information about the DPF. It has also published guidance, including in the form of FAQs addressed to individuals, as well as to EU and U.S. businesses[27]. The EDPB has in turn developed complaint forms and FAQs addressed to individuals and businesses. Similarly, the Commission published a Q&A and factsheet on the DPF when it adopted its adequacy decision[28].

At the same time, it emerged from the review meeting that more work is needed to raise awareness among individuals and provide guidance to companies. The input received from companies and IRMs, and very low number of complaints suggests that individuals may not always be aware of their rights and/or the mechanism to exercise them. During the review meeting, the DoC expressed an interest in working together with the EU DPAs to increase awareness of the Framework among EU individuals. The Commission encourages such initiatives and is also taking steps to better inform individuals, including by providing additional information on the DPF on its website, for instance by incorporating links and references to relevant guidance documents adopted by the EDPB, DoC and other U.S. authorities.

When it comes to guidance on the DPF Principles, EDPB representatives agreed during the review meeting to cooperate in the coming months to provide further clarifications about the notion of HR data under the DPF and the specific obligations that apply to the processing of such data. Different elements to be included in such guidance were explored. For example, this

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] See e.g. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

guidance could address certain practical scenarios where employee data would be processed under the DPF (e.g. by a cloud provider) and explain for such scenarios which DPF obligations would be relevant. Moreover, it could suggest companies that receive employee data of EU individuals (but do not necessarily use such data in the context of an employment relationship) to choose the DPA panel as their IRM. This would ensure that those individuals can turn to an authority that is 'close to home' and, where necessary, is more familiar with applicable national laws that apply to HR data.

In addition, a specific aspect where it seems that more guidance would be useful (also based on input received from trade associations) concerns the DPF requirements for onward transfers. Moreover, the DoC indicated that it would be worth exploring whether some sectors may benefit from additional guidance on the application of the DPF Principles to their activities, e.g. in the area of health research and financial services.

The Commission welcomes the readiness of both sides to develop guidance and expects that the work on the abovementioned topics will start soon.

More generally, several mechanisms have been set up to ensure exchanges and cooperation between U.S. authorities and the DPAs, including through the appointment of dedicated contact points within the FTC and DoC to deal with inquiries and referrals from DPAs.

2.1.5. Relevant developments in the U.S. legal system

Since the adequacy decision was adopted, there have been a number of developments in the U.S. legal framework in the area of privacy. This includes legislative, regulatory and case law developments. They generally signal an increased convergence between the EU and the U.S.'s approaches to certain challenges to privacy, including through the use of similar legal concepts. Certain of these developments are ongoing and will require to be further monitored.

At federal level, the President issued several Executive Orders (EOs) that are relevant for the use of personal data. In particular, Executive Order 14117 of 28 February 2024[29] prohibits or limits transactions involving certain categories of sensitive personal data (e.g. health data, biometric identifiers, human genomic data) with entities in some "countries of concern"[30]. The order adopted instructs the Attorney General to propose regulations – still to be issued at the time of the adoption of the present report – to further specify its implementation. In addition, Executive Order 14110 of 30 October 2023 on artificial intelligence[31] focuses on the development of safe, secure and trustworthy artificial intelligence. It requires several federal agencies to develop AI-related safety standards and guidelines, including on specific AI risks for privacy and on privacy-preserving techniques.

In terms of legislative work, while federal privacy bills have been introduced in Congress over the past years, 20 U.S. States have enacted comprehensive privacy laws as of July 2024, of which eight have entered into application: California, Colorado, Oregon, Virginia, Connecticut,

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] These include, as proposed by the Attorney General in an Advance Notice of Proposed Rulemaking issued on 3 May 2024, China, Cuba, Hong Kong and Macau, Iran, North Korea, and Venezuela. See https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

Utah, Texas and Florida. Moreover, 17 U.S. States have adopted legislation addressing automated processing (or, at least, some forms of it) and generally allowing opt-outs for certain types of decision-making based on "profiling"[32].

In terms of case-law developments, several civil society representatives have pointed to the recent judgment of the Supreme Court in *Loper Bright Enterprises v. Raimondo* (of 28 June 2024). This judgment overrules previous case law on the *Chevron* doctrine, whereby courts 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. In particular, some NGOs have expressed concerns about the impact of this Supreme Court ruling on the FTC's rulemaking authority in the area of privacy, while recognising that there may be no or limited impact on its enforcement powers. At the review meeting, the FTC informed that it is still early days to know the exact implications of this judgment. At the same time, it explained that FTC rule-making is done under an authority in the FTC Act different than those for other administrative agencies and for which the *Chevron* doctrine was less relevant. The recent judgment may therefore have limited impact in this area.

In addition, the FTC informed about recent developments in its approach to automated processing and artificial intelligence. This includes the adoption of a joint statement together with other enforcement authorities against discrimination and bias in automated systems[33], as well as several enforcement actions – in which the FTC focuses among other things on transparency, the fairness of automated processing and the ability of individuals to challenge outcomes. The most notable case in this respect is the FTC's decision against *Rite Aid* in March 2024, which imposed a 5-year ban on the use of facial recognition technology for security purposes by that company[34]. In particular, the FTC found that *Rite Aid* failed to take reasonable measures to prevent erroneous results and inform consumers of the technology used. More generally, at the review meeting, the FTC addressed its current priorities and notably the areas that it believes deserve a more proactive enforcement approach moving forward. This includes

[32] While there are differences in what is meant by "profiling" between the different States, profiling is generally defined as any form of automated processing performed on personal data to evaluate, analyse, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. It is typically consumers that can opt-out for profiling. The following States have developed legislation on profiling: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, enacted May 9, 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, enacted June 29, 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051), and Virginia (Va. Code Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

the protection of sensitive data (e.g. health data, biometric data, geolocation)[35], the protection of children[36] and minors online, and data security.[37]

The Commission will continue to closely follow these and other developments in the U.S., in particular any further steps towards a comprehensive federal privacy law and the possible impact of the Supreme Court's recent case law on the FTC's role in the area of privacy.

The Commission welcomes the information provided by the FTC on its recent enforcement activities and current priorities that largely correspond to trends and priorities in data protection enforcement in Europe. The FTC is also taking an active part in the network that brings together countries benefiting from an EU adequacy decision, which the Commission launched in March 2024[38]. This increased convergence should encourage and facilitate closer cooperation between privacy enforcers on both sides of the Atlantic, notably on matters relevant to the functioning of the DPF.

2.2. Aspects relating to access and use of personal data transferred under the EU-U.S. Data Privacy Framework by U.S. public authorities

The adequacy decision contains a detailed assessment of the rules that govern the collection and use of personal data transferred from the EU to DPF-certified companies by U.S. public authorities, in particular for criminal law enforcement and national security purposes. Since the adoption of the adequacy decision, as confirmed by the U.S. authorities during the review meeting, there have been no relevant developments with respect to the legal framework that applies to access to data for law enforcement or regulatory purposes in the first year of the DPF. For this reason, the below findings only concern developments in the area of national security.

The conclusions reached in the adequacy decision on access to data by intelligence agencies rely on the analysis of the conditions and limitations that apply to signals intelligence operations under several relevant legal authorities – in particular Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 [39] – as complemented and strengthened by the Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence (EO 14086) adopted by the U.S. President on 7 October 2022. The safeguards laid out in EO 14086 apply to all U.S. signals intelligence activities, regardless of the legal authority on which such activities are based and of where they take place, and protect the data of non-

[35] See e.g. the recent FTC's Order against X-Mode for Selling and Sharing Sensitive Location Information (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) and against Monument regarding Disclosures of Sensitive Health Data to Third Parties for Marketing Purposes (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] For example, the FTC has recently announced an investigation leading to a lawsuit against TikTok and its parent company, Bytedance, for allegedly infringing children's privacy law. It is alleged that both companies failed to comply with the requirement to notify and obtain parental consent before collecting and using personal information from children under the age of 13 (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] See overview of recent enforcement activities in the FTC 2023 Privacy and Data Security Update: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] See https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. As a result of the March 2024 meeting, it was decided to hold a series of thematic sessions. The first one took place in July 2024 and focused on developing tools that can support small and medium enterprises in complying with privacy laws.

[39] Other measures that can be taken under FISA with respect to data transferred from the EU are individualised electronic surveillance (Section 105 FISA), physical searches (Section 302 FISA), the use of pen registers or trap and trace devices (Section 402 FISA) and the collection of business records from certain companies (common carriers, public accommodation facilities, vehicle rental facilities or storage facilities, Section 501 FISA). These different legal bases are analysed in detail in the adequacy decision (recitals 142-152).

U.S. persons (including Europeans)[40]. EO 14086 also established a new redress mechanism through which these binding safeguards can be invoked and enforced by individuals in the EU.

The next sections describe the steps taken by U.S. authorities since the adoption of the adequacy decision to comply with EO 14086, as well as relevant developments in relation to the abovementioned legal framework.

2.2.1. Relevant developments with respect to the U.S. legal framework

2.2.1.1. Implementation of Executive Order 14086 by intelligence agencies

The limitations and safeguards introduced by EO 14086 supplement those provided by Section 702 FISA and EO 12333. They are binding on all intelligence agencies and have been further operationalised through policies and procedures adopted by each agency.

As part of the first review, the U.S. authorities confirmed that there have been no changes to EO 14086 since its adoption. In addition, it was clarified that the U.S. President has not made use of the power envisaged in Sections 2(b)(i)(B) and 2(b)(ii)(C) of EO 14086 to update the list of legitimate objectives for which signals intelligence may be pursued or the list of purposes for which data collected in bulk may be used[41]. To determine more specific intelligence priorities for which signals intelligence may actually be collected, EO 14086 put in place a specific procedure. In particular, the ODNI Civil Liberties Protection Officer (ODNI CLPO) must be consulted to assess for each priority whether (1) it advances one or more legitimate objectives listed in the EO; (2) it was neither designed nor anticipated to result in signals intelligence collection for a prohibited objective listed in the EO and (3) it was established after appropriate consideration for the privacy and civil liberties of all persons[42]. The ODNI CLPO confirmed during the review meeting that she reviewed the priorities proposed by the Director of National Intelligence in the 2023 National Intelligence Priorities Framework, concluded that they complied with the above requirements, and shared her conclusion with the Director of National Intelligence (DNI), who in turn submitted the priorities for validation to the President. The ODNI CLPO also provided training on the requirements of EO 14086 to parts of the intelligence community involved in developing intelligence priorities.

In addition, U.S. authorities have taken further practical steps in the past year to implement EO 14086 in their day-to-day operations. In particular, intelligence agencies have put in place further internal policies and guidelines on the application of the EO, for instance internal processes (through internal authorisation requirements, documented access controls so only those individuals who have been properly trained and have the necessary mission requirements have access to the information, etc.) to ensure that its necessity and proportionality requirements are complied in the context of both targeted and bulk collection[43]. Moreover, training on EO 14086 has been provided to staff of different intelligence agencies (e.g. NSA, CIA, FBI), including annual and ad hoc training sessions organised by the ODNI CLPO and mandatory trainings for all new staff joining ODNI.

---

[40] See for further information section 3.2.1.2 of the adequacy decision.

[41] These legitimate objectives/purposes include, for instance, protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, or on behalf of, or with the assistance of a foreign government, organisation or person; protecting against terrorism, the taking of hostages, and the holding of individuals captive conducted by or on behalf of a foreign government, organisation or person.

[42] Section 2(b)(iii) EO 14086

[43] See https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, published on 3 July 2023.

The Commission welcomes the various measures put in place to implement and ensure compliance with EO 14086. As more experience is gained with the practical application of the EO's safeguards, the Commission would appreciate the opportunity to discuss concrete examples of how the EO is applied in practice (while respecting applicable confidentiality considerations) in future reviews.

2.2.1.2. Reauthorisation of Section 702 FISA

Section 702 FISA allows the targeting of non-U.S. persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information. The acquisition takes place on the basis of annual certifications submitted to and approved by the Foreign Intelligence Surveillance Court (FISC). These certifications identify specific categories of foreign intelligence to be collected. On 21 July 2023, ODNI announced that there are three approved certifications under Section 702 FISA, covering the following categories of foreign intelligence: (1) foreign governments and related entities, (2) counterterrorism, and (3) combatting proliferation[44]. The certifications are also required to include targeting and minimisation procedures that are approved by the FISC[45]. In particular, targeting is carried out by requesting that U.S. companies meeting the FISA definition of 'electronic communication service provider' disclose electronic communications data for communications sent to or from 'selectors', which identify a specific communication account, e.g. a telephone number or an email address. The U.S. government has published a number of materials on Section 702 FISA to inform the public about the functioning of surveillance programmes, applicable requirements and privacy protections as well as the role of the FISC[46].

Due to a sunset clause, Section 702 FISA was set to expire at the end of 2023, unless re-authorised by Congress. After a temporary re-authorisation without any changes, Congress passed the Reforming Intelligence and Securing America Act (RISAA) on 19 April 2024, re-authorising Section 702 FISA for a period of 2 years and introducing several changes. These can broadly be divided into two categories: (1) changes in the scope of surveillance activities allowed under Section 702 FISA and (2) institutional and procedural changes.

Changes in the scope of surveillance activities allowed under Section 702 FISA

RISAA has introduced three main changes to the scope of surveillance activities that can be carried out under Section 702 FISA.

First, 'abouts' collection has been definitively prohibited[47]. This refers to the collection of communications where the Section 702 selector (such as an email address) is not in the 'to' or 'from' of the communications, but rather contains a reference to such a selector in the communication (e.g., email communications that are not sent to or from the selected email address, but include the selected email address in the email text or body). While such collection was already excluded following an amendment to FISA in 2018, FISA still provided for the possibility to restart 'abouts' collection in the future, following a specific authorisation

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Such procedures limit the collection of data with respect to a specific foreign intelligence purpose, restrict access to databases in which information acquired under Section 702 FISA is stored (including through access controls) and impose limits on the use, retention and dissemination of such information.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.
[47] Section 22 RISAA.

procedure involving the FISC and Congress. The latest amendment introduced by RISAA has removed this possibility.

Second, the definition of foreign intelligence information has been expanded to include information relating to counternarcotics[48]. During the review meeting, the U.S. authorities explained that this was introduced in light of the current fentanyl crisis and the increasing national security threat from international narcotics traffickers and manufacturers. Against this background, it was confirmed that this notion falls under several of the legitimate objectives listed in EO 14086, i.e. understanding or assessing the capabilities, intentions, or activities of foreign organisations that pose a current or potential threat to the national security of the U.S. or its allies; understanding or assessing transnational threats that impact global security, including public health risks; and protecting against transnational criminal threats[49].

Third, RISAA expanded the definition of 'electronic communication service provider' (ECSP), thereby broadening the scope of companies that may be compelled to provide information pursuant to Section 702 FISA[50]. The definition now includes other service providers having "access to equipment that is being or may be used to transmit or store wire or electronic communications", while explicitly excluding public accommodation facilities, dwellings, community facilities and food service establishments. In a letter to Congress, the DoJ referred to this amendment as a technical change intended to cover an "extremely small" number of technology companies that, according to recent FISC and Foreign Intelligence Surveillance Court of Review (FISCR) decisions, were not captured by the previous definition of ECSP[51]. In that same letter, the DoJ committed to narrow down the scope by applying this definition exclusively to cover the type of service provider at issue in the litigation leading to the FISC decision. As a consequence, the companies concerned are named in a classified annex for Congress. Several NGOs, including those that provided feedback as part of the review, expressed concerns about this expansion arguing that it could potentially cover many U.S. businesses (since many of them provide some type of service and have access to communications equipment). In light of such concerns, a further amendment has been proposed with the support of the Intelligence Community in a draft Intelligence Authorisation Act for Fiscal Year 2025, which is currently before Congress. This change, if passed by Congress, would ensure that the additional companies captured by the definition of ECSP would only be limited to those mentioned in abovementioned FISC rulings. The bill also envisages that each directive addressed to such a company would have to be reported to the FISC, to allow the latter to review whether the company would indeed fall within the scope. In its letter to Congress, the DoJ committed to report to Congress every six months regarding any application of the updated definition in order to allow Congress to exercise the appropriate oversight as regard the narrow application of the definition.

Importantly, it was confirmed at the review meeting by the U.S. authorities and the PCLOB that all safeguards of EO 14086 continue to fully apply to all data collection and use under Section 702 FISA, including following these amendments. Thus, while the RISAA somewhat

[48] Section 23 RISAA.
[49] Section 2(b)(ii)(A)(2), (3) and (10) EO 14086.
[50] Section 25 RISAA.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. See the decision of the FISC of 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) and the ruling of the Foreign Intelligence Surveillance Court of Review upholding that decision (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

broadens the scope of companies that may get an order, it does not limit the exercise of rights. Nevertheless, it will be important to monitor further (legislative and reporting) developments and receive information on the application of these new rules in practice. This includes for instance the impact of the broadening of the definitions of foreign intelligence and ECSPs on the number of Section 702 FISA targets (as communicated annually by the ODNI, see below on transparency). The future follow-up report to the recent PCLOB report on Section 702 FISA (see below) should be particularly informative in this regard.

Institutional and procedural changes

In terms of institutional and procedural changes, RISAA codified several procedures that were already followed in practice and introduced new safeguards. While some of these only concern U.S. persons, several changes increase protections for both U.S. and non-U.S. persons whose data may be collected under Section 702 FISA[52] and are therefore relevant to the functioning of the DPF.

First, a number of additional accountability, oversight and reporting requirements were put in place. In particular, FBI personnel must now be trained annually on the rules that apply to the querying of information obtained under Section 702 FISA[53]. The FBI is also required to report to Congress on its querying activities (e.g. the number of queries using 'batch job technologies', i.e. running multiple query terms as part of a single query) and on accountability measures put in place to ensure compliance with legal querying requirements (Sections 11-12 RISAA). Moreover, the Inspector General of the DOJ is instructed to produce a report on FBI compliance with querying requirements (Section 9 RISAA). More generally, to increase the transparency of procedures before the FISC, ODNI and the Attorney General are now required to complete declassification review of FISC decisions within 180 days (Section 7 RISAA). In addition, transcripts of all hearings before the FISC and the Foreign Intelligence Court of Review (FISCR, where FISC decisions may be appealed) must be kept and transmitted to Congress (Section 8 RISAA).

Second, RISAA introduced further limitations on the use by the FBI of data collected under Section 702 FISA. Section 2(d) RISAA provides that a query using 'batch technology' can only be done after obtaining approval from an attorney within the FBI, unless there are exigent circumstances. In addition, the FBI is now prohibited from automatically checking unminimised information acquired under Section 702 FISA and instead has to ensure that analysts have to affirmatively select to search against such information. RISAA has also prohibited the FBI from conducting queries that are solely designed to find and extract evidence of criminal activity (unless there is a reasonable belief that they could assist in mitigating or eliminating a threat to life or serious bodily harm, or where necessary to comply with disclosure obligations in litigation)[54]. Moreover, the FBI is prohibited from ingesting un-minimised data

[52] In addition, RISAA introduced some changes with respect to traditional individualised electronic surveillance pursuant to Section 105 FISA (on the basis of FISC warrant issued if a standard of probable cause is met). An application by an intelligence agency to the Attorney General for an order to conduct individualised electronic surveillance now requires a sworn statement justifying the belief that the conditions of Section 105 FISA are met (Section 6(a) RISAA). The possible duration of electronic surveillance with respect to foreign powers or agents of foreign powers has been extended from 120 days to 1 year (Section 6(g) RISAA).

[53] Section 2(d) RISAA.

[54] Section 3(a) RISAA.

into analytic repositories unless the targeted person is relevant to an existing national security investigation[55].

Third, certain provisions relating to the status and role *amici curiae* before the FISC have been changed[56]. The *amici* are designated as experts to assist the Court (and the FISCR) on matters related to privacy and civil liberties or to help clarify technological issues when dealing with a specific government's application. Whereas FISA previously required that *amici* had expertise in privacy and civil liberties, intelligence collection, communications technology or other relevant areas, it now requires, in principle, expertise in privacy/civil liberties and intelligence collection. The Court already had the possibility to appoint an *amicus* in any instance it deemed appropriate, and was required to do so when dealing with a novel or significant interpretation of the law. Following the reauthorisation, the FISC is now also required to appoint an *amicus* each time it is asked to approve a Section 702 FISA certifications and accompanying procedures (e.g. targeting procedures), unless it finds that this would not be appropriate or likely result in undue delay[57]. In addition, instead of appointing just one, the Court can decide now to appoint one or more *amici*. It is also clarified that information to be provided by *amici* must be "limited to addressing the specific issues identified by the court", although the areas on which the *amici* may comment have remained broad (i.e. legal arguments and information related to the protection of individual privacy and civil liberties of United States persons, intelligence collection and communications technology or any other relevant area).

Finally, Section 18 RISAA establishes a 'FISA Reform Commission' – consisting among others of Congress Members, the PCLOB Chair, Principal Deputy Director of National Intelligence, and the Deputy Attorney General, and additional members to be appointed by Congress[58] – to recommend additional FISA reforms.

The Commission will closely monitor further developments with respect to Section 702 FISA, including in the context of oversight activities of the PCLOB (see below), the work of the Reform Commission and the upcoming review of FISA after 2 years.

2.2.1.3. Surveillance activities in practice: figures and trends

The ODNI's Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities for Calendar Year 2023 (published in April 2024)[59] shows that the number of targets under Section 702 FISA increased from 245 073 in calendar year 2022 to 268 590 in calendar year 2023. The report explains that fluctuations in the number of targets may be linked to a variety of reasons, including changes in operational priorities, world events, technical capabilities, target behaviour, and changes in the telecommunication sector. The report also indicates that no non-US persons (compared to 1 in 2021 and 0 in 2022) were targeted under Section 402 FISA (pen register and trap and trace), whereas six orders (compared to 11 orders in both 2021 and 2022), for six targets (compared to 13 in 2021 and 11 in 2022), were issued under Section 501 FISA (access to business records of common carriers, vehicle rental facilities or physical storage facilities), covering 5412

[55] Section 3(b) RISAA. Where necessary due to exigent circumstances, the FBI Director can decide on an exception to this provision, which has to be notified to Congress.
[56] For sake of clarity, these amendments do not affect the status and role of the special advocates before the DPRC, as confirmed by the U.S. at the review meeting.
[57] Section 5(b) RISAA.
[58] Section 18 specifically requires representation from outside of Congress.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

unique identifiers (compared to 23,157 in 2021 and 55,431 in 2022) used to communicate information collected pursuant to such orders.

The DoJ's annual Foreign Intelligence Surveillance Act report to Congress indicates that, during calendar year 2023, 327 applications were filed with the FISC to conduct electronic surveillance and/or physical searches for foreign intelligence purposes under Section 105 and 302 FISA respectively[60]. The total number of targeted persons was between 500 and 999. As regards national security letters (NSLs), the report provides that 10 115 requests (excluding requests for subscriber information only) were issued for information on non-U.S. persons, seeking information pertaining to 3033 different non-U.S. persons[61].

Several DPF-certified companies (e.g. Google, Meta) make use of the possibility provided under U.S. law to publish transparency reports that inform about the number of FISA and NSL requests they have received during a given reporting period. At the time of drafting this report, the statistics on FISA requests after July 2023 were not yet available. Google for example reported to have received 500 to 999 NSLs requests, affecting 2000 to 2499 accounts, between July and December 2023[62]. Meta reported that it received 0 to 499 NSL requests, affecting 500 to 999 accounts, in the same reporting period[63]. The numbers have remained rather stable in recent years. To further increase transparency, some companies (e.g. Google) proactively publish NSL they have received once non-disclosure restrictions are lifted[64].

2.2.1.4. Other developments

In the context of the preparation of the review, several NGOs have raised questions on new forms of data acquisition by U.S. intelligence agencies through the purchase of data from commercial entities, in particular data brokers. They explained that while data collected on this basis must still be processed in accordance with other requirements, including for example under EO 12333[65], such acquisition takes place outside the framework of FISA and EO 14086.

In this respect, it should be recalled that any type of voluntary sharing of data with third parties is subject to several detailed conditions under the DPF. First, certified organisation cannot share data with a third party (not acting as an agent/processor) without providing notice and choice to the individuals concerned[66]. Second, in accordance with the *Accountability for Onward Transfers Principle*, onward transfers may only be carried out (1) for limited and specified purposes, (2) on the basis of a contract between the EU-U.S. DPF organisation and the third party and (3) only if that contract requires the third party to provide the same level of protection as the one guaranteed by the Principles[67].

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] These figures have remained largely stable in comparison to the previous reporting year (2022). By comparison, in 2022 there were 317 final applications with the FISC to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The total number of persons targeted for orders for electronic surveillance was between 0 and 499. The FBI made 9103 NSL requests for information on non-US persons in 2022 (excluding requests for subscriber information only). Source: https://irp.fas.org/agency/doj/fisa/2022rept.pdf
[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] See for instance section 2.4 of EO 12333 on collection techniques.
[66] See recital 40 of the adequacy decision.
[67] See recital 38 of the adequacy decision.

Furthermore, as also discussed during the review meeting, the FTC has taken enforcement actions against data brokers selling sensitive consumer data. For instance, in a case against *X-Mode* and its successor *Outlogic*, the FTC adopted an order on 9 January 2024 prohibiting the company from selling geolocation data to third parties and deleting data it had used and shared unlawfully. The FTC's investigation found among other things that the company did not fully inform individuals about the use and sale of their geolocation data, failed to put in place measures to allow individuals to opt-out of tracking, allowed the use of the data for potentially discriminatory purposes and failed to put limits to the use of such information by third parties[68]. The Commission expects the same approach will be adopted by the FTC if DPF certified companies were to share data in violation of the above-mentioned provisions.

Finally, it is worth mentioning that in May 2024, ODNI issued the Intelligence Community Policy Framework for Commercially Available Information[69]. This Framework lays down a number of principles and requirements that intelligence agencies should follow, including to minimise privacy and civil liberties' risks, when acquiring and using information in the context of a commercial transaction.

2.2.2. Independent oversight

The activities of U.S. intelligence agencies are subject to supervision by different bodies, including Privacy and Civil Liberties Officers, Inspectors General, Congress and the PCLOB. In particular, EO 14086 requires each intelligence agency to have senior-level legal, oversight and compliance officials to ensure compliance with applicable U.S. law. This oversight function is fulfilled by officers with a designated compliance role, as well as Privacy and Civil Liberties Officers and Inspectors General[70]. They must conduct periodic oversight of signals intelligence activities and ensure that any non-compliance is remedied. Intelligence agencies must provide such officials with access to all relevant information to carry out their oversight functions and may not take any actions to impede or improperly influence their oversight activities.

The General Counsel of the Office of the Intelligence Community Inspector General (ICIG) in the ODNI – which has comprehensive jurisdiction over the entire Intelligence Community and is authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority – participated in the review meeting. He confirmed that the ICIG systematically checks compliance with EO 14086 as part of its oversight activities. He also referred to recent oversight activities of other Inspectors General of the intelligence community, as detailed in regular reports. For example, in its semi-annual report to Congress for April-

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Intelligence agencies are required to comply with the Framework since August 2024.

[70] Each intelligence agency has an Inspector General who is statutorily independent and responsible for conducting audits and investigations relating to the activities carried out by the respective agency for national security purposes. They have access to all relevant (including classified) material, if need be by subpoena, and may take testimony. Inspectors General refer cases of suspected criminal violations for prosecution and make recommendations for corrective action to agency heads. While their recommendations are non-binding, their reports, including on follow-up action (or the lack of it) are generally made public and sent to Congress. See in this regard footnote 136 of the adequacy decision on the role of the Inspector General.

September 2023[71], the Inspector General of the NSA informed about an evaluation of an internal NSA control framework for targeting decisions and requests. It concluded that this framework was functioning properly to ensure compliance with the laws, directives and policies that protect civil liberties and privacy. The same report also mentions an investigation that revealed the misuse of a signals' intelligence tool for unauthorised purposes by an NSA employee.

Under EO 14086, the PCLOB[72] is entrusted with specific oversight functions[73]. The Chair of the PCLOB and its three members participated in the review meeting, and informed that the PCLOB provided advice to intelligence agencies on their draft policies and procedures implementing EO 14086 in April 2023, and was consulted on the nomination of the Data Protection Review Court (DPRC) judges and special advocates. The Board also launched an oversight project to (1) review the implementation of the updated policies and procedures adopted by the intelligence agencies to ensure that they are consistent with the EO, and (2) conduct an annual review of the functioning of the new redress mechanism (see below)[74]. The PCLOB Members confirmed that the Board plans to carry out both reviews in the near future. With respect to the redress, they explained that, in the absence of complaints, the PCLOB's review will focus on the policies and procedures put in place to set-up the mechanism.

In terms of other oversight activities, the PCLOB issued a report on Section 702 FISA on 28 September 2023[75]. This report is a follow-up to an earlier report of 2014 and contains updated factual and legal information on the operation of Section 702 FISA surveillance programmes. The report also contains recommendations on compliance by intelligence agencies with applicable requirements and suggestions to Congress to further strengthen several aspects of Section 702 FISA in the context of its reauthorisation (including by codifying the legitimate objectives for surveillance activities listed in EO 14086).[76] During the review meeting, the PCLOB informed that it expects to receive soon responses from intelligence agencies on the implementation of its recommendations, which will feed into a future follow-up report. Other ongoing oversight projects include one on countering domestic terrorism and its impact on privacy and civil liberties and the collection of open-source or commercially available data by the FBI[77].

---

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] The PCLOB is an independent agency entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view in order to protect privacy and civil liberties. It can access all relevant (including classified) information, conduct interviews and hear testimony. It may issue recommendations to the law enforcement and intelligence authorities, and regularly reports to Congress and the President. Its reports are made publicly available to the greatest extent possible.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] The Commission notes that some of those recommendations have been incorporated as part of RISAA, including the recommendation on the abouts collection or the recommendation on strengthening of the role of the FISC experts (amici).

[77] https://www.pclob.gov/OversightProjects.

Finally, NGOs consulted in the context of the review, expressed the concern that the term of several PCLOB Members is set to expire in the near future, potentially leaving the PCLOB without a quorum. In particular, the term of the Chair has expired and the period during which she can serve in a holdover capacity ends in January 2025, while another seat is vacant, and a third one will vacate also in January of next year. During the review meeting, the Members explained that they do not expect the PCLOB to end up without a quorum, since a nomination has already been issued for the seat that is currently vacant (and is awaiting Senate confirmation)[78]. They also underlined that, even if the Board would lose its quorum, this would not affect its capacity to continue carrying out oversight projects. Nevertheless, given the important role of the PCLOB to review the implementation of EO 14086, the Commission will closely monitor the status of future vacancies and nominations/appointments.

2.2.3. Redress

EO 14086, complemented by a Regulation of the Attorney General, established a new redress mechanism to handle and resolve qualifying complaints from individuals concerning U.S. signals intelligence activities[79]. Any individual in the EU is entitled to submit a complaint to the redress mechanism concerning an alleged violation of U.S. law governing signals intelligence activities (e.g. EO 14086, Section 702 FISA, EO 12333) with respect to personal data transferred to the U.S. that adversely affects their privacy and civil liberties interests. Individuals can submit a complaint with a DPA in an EU Member State, which channels, via the secretariat of the EDPB, the complaint to the redress mechanism. The mechanism consists of two layers, with the initial investigation of complaints carried out by the ODNI CLPO and a possibility for individuals to appeal the CLPO's decision before an independent DPRC. Once a review by the ODNI CLPO or DPRC is completed, individuals are informed, through the national authority, that "the review either did not identify any covered violations or the ODNI CLPO/the DPRC issued a determination requiring appropriate remediation". Decisions of the ODNI CLPO and DPRC are binding on intelligence agencies.

Since the adoption of the adequacy decision, further steps have been taken to make the redress mechanism fully operational.

As regards the establishment of the DPRC, on 14 November 2023 eight judges (i.e. two more judges than the minimum number required under EO 14086, as complemented by the Attorney General's regulations at 28 C.F.R. § 201.3(a)) were appointed to the court[80]. They were appointed on the basis of the criteria set out in EO 14086 and in accordance with the process established therein, including after consultation of inter alia the PCLOB[81]. They include former federal District Court and Court of Appeals' judges, a former U.S. Attorney General and a former member of the PCLOB. As required by the EO, at least half of the judges have prior judicial experience. In addition, in April 2024, two special advocates – legal practitioners with an expertise in both privacy and national security – have been appointed to represent the interests of individuals before the DPRC. It was confirmed at the review meeting that all judges and special advocates have received the highest security clearance and can therefore have access to classified materials when performing their tasks for the DPRC. The DPRC had also

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Recitals 176-194 of the adequacy decision.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Section 3(d)(A) EO 14086.

published a series of Frequently Asked Questions, providing more information on its role, independence and functioning[82].

Concerning the handling of complaints, the ODNI adopted on 6 December 2022 Intelligence Community Directive 126, which regulates in detail (by setting deadlines, establishing a secure electronic repository and communication channels, requiring CLPO and Intelligence Community elements to cooperate with the PCLOB in the context of the annual review of the redress mechanism, etc.) different aspects of the process for the investigation and adjudication of complaints[83]. This Directive is applicable across the U.S. Intelligence Community and has been complemented by further internal procedures adopted by individual intelligence agencies on their cooperation with the ODNI CLPO in the context of the handling of a complaint (e.g., development of secure repository for sharing complaints and responsive documents; and secure communications between the relevant agencies). The DPRC will also issue in the coming months more detailed rules on the handling of complaints and other procedural aspects.

A number of additional measures were taken in the European Union and the United States to inform the general public, as well as facilitate the submission and handling of complaints. This includes the adoption by the EDPB of an information note on the new redress mechanism[84], a template complaint form (that is intended to be translated and published by all DPAs in their national languages)[85] and rules of procedure that govern the cooperation between national supervisory authorities and the EDPB secretariat[86]. Similarly, the ODNI published FAQs and a fact sheet on the new redress mechanism, and engaged in public awareness raising activities[87].

Furthermore, over the past year, the EDPB and the relevant U.S. authorities have cooperated closely on several operational aspects. In particular, as confirmed during the review meeting, they put in place an encrypted communication channel to transmit complaints from national authorities in the EU to the EDPB secretariat, from the EDPB secretariat to the ODNI CLPO as well as to the DoJ Office of Privacy and Civil Liberties (OPCL), and between the ODNI CLPO and other authorities on the U.S. side (e.g. the DPRC). In addition, the ODNI CLPO explained that further internal procedures have been put in place for the cooperation of individual intelligence agencies with the ODNI CLPO as regards the handling of a complaints.

Finally, the OPCL, which provides administrative support to the DPRC, also informed that the DPRC operates under its own dedicated budget line and is provided with the necessary facilities to carry out its tasks, including secure computers and laptops, phones, etc. In addition, as required by EO 14086, the DoC has taken the necessary measures, including by setting up an encrypted communication channel with the ODNI CLPO, to maintain a record of all qualifying complaints received. The DoC will periodically contact ODNI CLPO regarding whether

[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf and https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

information relating to an individual complaint has been declassified. If so, the DoC will notify the concerned individual thereof, to allow him or her to obtain access to such information.

At the time of the review meeting, no complaints had been received by EU supervisory authorities and the new redress mechanism had therefore not been triggered yet.

3. CONCLUSION

Based on the information gathered during this first review, the Commission concludes that the U.S. authorities have put in place the necessary structures and procedures to ensure that the Data Privacy Framework functions effectively. In this context, the Commission very much values the very good cooperation with the U.S. authorities to conduct the review.

While this first review naturally focused on verifying whether all the constitutive elements of the framework are in place, experience with the practical application of the safeguards applying both to the processing of data by certified companies and to access to data by public authorities is necessarily limited after just one year of operation. The Commission will therefore closely monitor relevant developments in the next months and years, paying particular attention to (1) the upcoming reports of the PCLOB on the implementation of EO 14086 and the functioning of the signals' intelligence redress mechanism, in particular the DPRC; (2) possible further amendments of Section 702 FISA; and (3) the nomination and appointment of members to the PCLOB to fill upcoming vacancies.

Moreover, to ensure a continued and effective functioning, the Commission considers it important that:

- As announced at the review meeting, the DoC makes fuller use of the different tools provided in the DPF for the monitoring of compliance by companies with the Principles and the detection of false claims of participation.
- The FTC further develops its proactive approach to the investigation and enforcement of compliance by certified companies with the DPF Principles; and
- The DoC, FTC and EU data protection authorities develop common guidance instruments on key requirements under the DPF Principles, e.g. on HR data and onward transfers.

In light of this outcome of the review and as envisaged in recital 211 of the adequacy decision, the Commission considers it appropriate to carry out the next periodic review after three years. This should allow more experience to be gained with the practical application of the DPF and take into account the abovementioned upcoming developments. The Commission will therefore, in accordance with Article 3(4) of the adequacy decision, consult the EDPB and the Committee established under Article 93(1) of the General Data Protection Regulation on the periodicity of future reviews.