EU - U.S. Privacy Shield - Third Annual Joint Review

Adopted on 12 November 2019

Table of contents

The European Data Protection Board

Having regard to Article 4 and Recitals 145 to 149 of the 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 ("EU - U.S. Privacy Shield),

HAS ADOPTED THE FOLLOWING REPORT:

1 EXECUTIVE SUMMARY

1.1 Introduction

1. According to the EU–U.S. Privacy Shield adequacy decision ("Privacy Shield")[1] adopted on 12 July 2016, **eight representatives of the EDPB participated in the third joint review conducted by the European Commission, on September 12 and 13 of 2019** in Washington to assess the robustness of its adequacy decision and its practical implementation.

2. Based on the concerns elaborated in the previous opinions of the WP29 and of the EDPB, in particular opinion 1/2016, and the reports following the first and second joint review, the EDPB focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU individuals.**[2] The EDPB assessed once again whether these concerns have been addressed and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.

3. The European Commission published its report of the third joint review on October 23, 2019.

4. **The EDPB's main findings concerning this third joint annual review**, stemming both from written submissions and from oral contributions are hereby presented in this report.

1.2 On the commercial aspects of the Privacy Shield

5. The third annual review showed that the U.S. authorities have continued their efforts to implement the Privacy Shield.

6. The **DoC as well as the FTC also undertook new ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield. The EDPB particularly welcomes that the DoC has increased the number of "random spot checks" to 30 organizations per month.

7. **However, one of the main concerns already expressed by the WP29 and the EDPB remains a certain lack of oversight in substance.** Indeed, the checks performed by the DoC are principally focused on formal aspects. The enforcement actions by the FTC focused on procedural violations of the framework

1 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

[2] Any reference to the "EU" shall be understood as a reference to the "EEA", in accordance with Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 and Decision of the EEA Joint Committee No 144/2017 of 7 July 2017.

rather than on the substance. **This lack of substantial checks thus remains a concern of the EDPB as, even taking into account discretionary and limited investigations by the FTC, a majority of companies' compliance with the substance of the Privacy Shield's principles remains unchecked, although many of them were introduced or further detailed compared to the Safe Harbor. In addition, the increase of complaints, in general, although resolved successfully, does not entirely compensate for this lack of proactive checks on substance. Indeed, these complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.**

8. **One example for which the EDPB sees the need for more substantive checks are onward transfers.** Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent US Authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle". As a first step, for example the DoC could make use of its right to ask organizations to produce the contracts they have put in place with third countries' partners in order to assess whether those provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed.

9. **Another area that requires further attention is the application of the Privacy Shield requirements regarding HR Data.** While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of EU data subjects.

10. **Also, the re-certification process needs to be further refined**. The situation of outdated listings leads to avoidable confusion that should be addressed also in the interest of concerned Privacy Shield certified organizations.

11. Last but not least, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the application of the principles when it comes to "processors", the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information. Those remain valid.

1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield

12. The EDPB **welcomes the appointments of the last missing members of the Privacy and Civil Liberties Oversight Board (PCLOB), enabling it to be fully functioning and operational, as well as its increased transparency concerning its work plan.**

13. **The EDPB also welcomes the appointment of Mr Keith Krach, as "permanent" Ombudsperson on 18 January 2019**.

14. Despite these developments, **some of the main points of concern, already expressed by the WP29 and the EDPB in this area in their previous reports, still have to be fully resolved**.

15. More specifically, the c**ollection and access of personal data for national security purposes** under both Section 702 of FISA[3] and Executive Order 12 333[4] still remains an important issue for the EDPB.

16. In this respect, the EDPB recalls that it continues to consider that within the surveillance programs, more specific safeguards would be needed, e.g. for precise targeting to determine whether an individual or a group can be a target of surveillance and for stricter scrutiny of individual targets by an independent authority ex-ante.

17. In addition, although it acknowledges the efforts that the PCLOB has undertaken to follow-up on its past recommendations concerning section 702 FISA, as well as to issue a new report on the FBI's querying of data under Section 702, **the EDPB deeply regrets that the PCLOB will not issue further reports** on PPD-28[5] to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a general updated report on Section 702 FISA, especially since it was reauthorized with few adjustments since the last Joint Review. The EDPB indeed recalls, as the WP29 did before, that reports of the PCLOB were very useful to feed the assessment led by the WP29 and by the EDPB and would in particular be useful to assess whether the collection of data under Section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of "targets", the tasking of selectors under **Section 702** (including in the context of the **UPSTREAM program**[6]), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB will welcome the finalization by PCLOB of its awaited reports on EO 12 333. However, as the EDPB understands that these reports will most likely remain classified, they may not be used as a relevant source of information on the concrete operation of this Executive Order and on its necessity and proportionality.

18. Access to such reports **would allow the EDPB to provide a comprehensive assessment of these aspects**. It consequently stresses that, in order to perform more meaningful reviews, it could benefit from accessing to additional documents and discussing additional classified elements, following the examples of PNR or TFTP reviews.

---

[3] See the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq.) (FISA) – its section 702 allows for data to be collected from non-U.S. persons reasonably believed to be outside the United States in order to obtain foreign intelligence information (50 U.S. Code §1881a (D)(1))

[4] See footnote 59 of the Privacy Shield Adequacy Decision: "E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981). To the extent that the Executive Order is publicly accessible, it defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities (in particular the need to promulgate specific procedural rules). According to Sec. 3.2 of E.O. 12333, the President, supported by the National Security Council, and the DNI shall issue such appropriate directives, procedures and guidance as are necessary to implement the order."

[5] "PPD-28 is a directive of the President of the United States laying down consistency principles with which signals intelligence collection shall be authorised and conducted but PPD-28 is not a legal basis for collection" – See Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision of the WP 29 as well as annex VI of the Privacy Shield Decision

[6] See WP29 report on the Privacy Shield of 28 November 2017 (page 15): "Two programs are confirmed to be operating under Section 702 of FISA: PRISM and UPSTREAM. (…)Under PRISM, the relevant U.S. authorities require internet service providers to provide them with the data of their users corresponding to "selectors", once "tasked" by the competent authority.
Under the UPSTREAM program, the providers of the telecommunication backbone are required to assist the NSA by identifying and collecting transiting data "to" and "from" a chosen "selector" in the flow of communications between communication service providers."

19. Due in particular to the problematic admissibility threshold of the **"standing requirement**", the redress by EU citizens before U.S. courts is still to be effectively guaranteed. Therefore, the EDPB will continue to follow closely the evolution of the case law.

20. Hence, the independence of the Ombudsperson remains a key element, as this institution is designed to compensate the uncertainty in seeking effective redress before the court, if not the lack thereof.

21. During the third annual review, it was clarified that any violation of the targeting and minimisation procedures under Section 702 FISA would be reported to the FISC by the Ombudsperson, in which case the FISC may decide to issue a deficiency order. Despite further discussions on the procedural aspects of the (inadmissible) first case referred to the Ombudsperson by the EU Centralized Body earlier this year, as well as on hypothetical cases which brought some clarifications, the exact powers of the Ombudsperson still need to be clarified, through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the intelligence community or oversight bodies. Based on the information provided so far, the EDPB is of the view that the Ombudsperson's access to information, which appears to remain indirect, and its powers to remedy non-compliance vis-à-vis the intelligence authorities, are still not sufficient in the light of Article 47 EU Charter of Fundamental Rights. It also underlines that the Ombudsperson is not in a position to bring a matter before the court other than to bring a violation of Section 702 FISA to the attention of the FISC.

22. Finally, regarding the **access to data for law enforcement purposes,** the EDPB underlines its remaining concerns on the available effective remedies for individuals in cases where the personal data processed by companies are accessed by law enforcement authorities.

1.4 Conclusion

23. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**

24. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

25. **As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and** the application of the principles when it comes to **processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

26. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets** that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. **The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the**

EDPB remain ready to review additional documents and discuss additional classified elements, in order to have **more meaningful reviews**, following the example of PNRs or TFTP reviews.

27. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

28. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending** before it.

2 INTRODUCTION

29. On 6 October 2015[7], the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.

30. On the 13 April 2016, the Working Party 29 issued an opinion[8] on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document[9] on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

31. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision[10].

32. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision[11] ("Privacy Shield"), which has also been incorporated into the EEA Agreement[12]. The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review[13]. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.

33. In addition, it is also foreseen in recital 147 of this adequacy decision that the Commission will meet a number of US authorities, and that the "*participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party*".

34. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017[14] as well as a second report following the second Joint Review in January 2019[15].

35. The third Joint Review of the Privacy Shield took place on the 12 and 13 September 2019 in Washington D.C. Eight representatives of the EDPB, a Commissioner as well as experts at staff level, were

7 Case C-362/14
8 WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
9 WP 237 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
10 EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf
11 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.
12 Decision of the EEA Joint Committee No 144/2017 of 7 July 2017 – Recital (1): "the 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 (1) is to be incorporated into the EEA Agreement".
13 See recitals 145-149 and Article 4(4) of the decision.
14 WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782
15 EU - U.S. Privacy Shield - Second Annual Joint Review - Adopted on 22 January 2019

designated to be part of the Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities, companies' representatives, NGOs and a representative from the binding arbitration mechanism.

36. In advance to the Joint Review, the Commission sent questionnaires to US trade associations representing Privacy Shield certified organizations and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The EDPB sent contributions to take part to the elaboration of these documents.

37. Right before the Joint Review, the Commission and the Review Team met with some of the NGOs to further discuss their input on the Privacy Shield.

38. Also, briefly before the actual Joint Review took place in Washington, the EU-Supervisory Authorities representatives were contacted by the DoC to informally discuss the existing divergences on the interpretation of the notion of HR Data (see I. 7.)

39. The new factual elements presented by the US authorities companies' representatives, NGOs and by a representative from the binding arbitration mechanism participating in the Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the EDPB Plenary on 8 October 2019.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

40. The EU-U.S. Privacy Shield is an adequacy decision that was designed to frame transfers of personal data outside the protections provided under GDPR to ensure the level of protection of natural persons guaranteed by GDPR is not undermined in the absence of a general law in the US providing for an essentially equivalent level of protection of personal data. It is of utmost importance that there is a common understanding of the text to ensure the application in the receiving State will correspond to the requirements for such transfers as set out under EU data protection law. It has to be ensured that this text is interpreted correctly and that organizations and individuals on both sides of the Atlantic are "on the same page" as regards their duties and rights under the Privacy Shield.

41. Thus, in the report of the first annual review the WP 29 emphasized the need for clear guidance on the application of the Privacy Shield principles. In the second year of operation of the framework and following informal consultation of members of the ITS at working level, the DoC has issued **guidance in the form of FAQs on the Accountability for Onward Transfer Principle**[16] **and the notion of Processor**[17] and published it on its website. In the third year of operation of the framework the DoC issued one more guiding document also in the form of FAQs on the Privacy Shield and the UK aiming at issues related to Brexit. The EDPB has not been involved in any way in the drafting of these new FAQs.

42. Since the last joint review, not much additional guidance was published by the US authorities. In this regard, the EDPB recalls in particular that guidance concerning processors may further specify the

16 https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs (last accessed on 18 December 2018)
17 https://www.privacyshield.gov/article?id=Processing-FAQs (last accessed on 18 December 2018)

application of the principles when it comes to processors ("agents").[18]. Also, the use of Standard Contractual Clauses as a tool for onward transfers remains to be examined.

43. The EDPB still regards the issuance of guidance as a good start and expects that in the future there will be more guidance as to other key elements. In previous reports, the EDPB already suggested to further work for example the **Choice Principle** (on when and how a data subject can opt out from the processing of his/her data for a new purpose), or on the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, it recalls that a **clarification of the scope of the right of access** could be helpful to prevent misunderstandings. In its last report, worries regarding the possibly very narrowly interpreted duty to grant the right of access only to data that is "stored" by an organization voiced by the WP 29 still remains valid.

3.2 Clear and easily available information for EU individuals

44. The WP 29 had found that to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies.**

45. The Privacy Shield website already had a specific section named "EU and Swiss individuals" containing subsections "My rights under Privacy Shield" and "Privacy Shield participants list"[19] where individuals were informed about their rights. The various possibilities to lodge complaints were also explained and partly supported by direct links. After the first annual review and as a response to the WP 29s suggestions the DoC added a one-page document to their website that gives individuals an overview[20] of the program with a strong focus on the individual's rights and how they can be exercised. The EDPB acknowledges the efforts made by the DoC to provide further guidance for EU individuals on the Privacy Shield website. Although the number of complaints slightly increased since the last report, it remains difficult to determine whether this is directly linked to this guidance. The EDPB will thus remain watchful.

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

46. After having noted improvements in the certification process in the report of the second Joint Review, the EDPB did not identify any relevant change of the procedures in the third Joint Review:

47. The DoC still reviews all self-certifications (both for first time applicants and for recertification submissions) and checks:

    1. Registration with an Independent recourse mechanism (IRM) company
    2. Payment of Annex I Arbitral Fund Contribution

18 that the guidance could for example further elaborate on the following details: Notice to be provided by processors needs to be in line with the contract in place between the processor and the controller; that access to data and a Choice mechanism could be provided to the individual directly by the processor provided however that the controller has in the first place authorized the processor to do so; and that for a processor compliance with the Data Integrity and Purpose Limitation principle requires it to process the data only in accordance with the instructions from the controller and on the other hand to implement the appropriate measures as instructed by the controller to assist the later in complying with the data integrity principle.
19 See: https://www.privacyshield.gov/Individuals-in-Europe (last accessed on 27 November 2018)
20 See: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq (last accessed on 14 December 2018)

3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
4. Completion and consistency of certification information
5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)

48. Also, the DoC still asks the organizations for more precise links provided for the Privacy Shield listing so individuals can more easily exercise their rights and for more than one point of contact within the organization to make sure messages from the DoC are received. The DoC also checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR).

49. When the DoC refused to list an organisation on the Privacy Shield list, either for first-time certifications or re-certifications, it underlined that it was because the requirements set out by the Privacy Shield were not fulfilled. This indicates that the decision made by the DoC whether or not to list an organization on the Privacy Shield website is – as far as the checks go - not a rubber stamp exercise.

50. However, on the basis of the information given by the US authorities during the joint reviews, those checks still do not go into the substance of the principles. **This absence of substantial checks remains a concern for the EDPB on the general question of sufficient oversight regarding the substance of the Privacy Shield principles.**

51. Following the criticism expressed by the WP 29, the DoC still prohibits a first-time applicant from making public representations about participation until the Privacy Shield Team approves its certification and instead requires an applicant to submit a draft privacy policy for review. It also directs an applicant to remove any premature references of their participation in the Privacy Shield program from their website.

52. **Regarding the re-certification process**, already the second annual review revealed that due to the procedures established by the DoC there are cases where the due date displayed on the Privacy Shield List is already passed while the organization still is listed as an active participant. This occurs when an organization has submitted their recertification but the process is not finalized before the due date. In the third review this was further explored and it was discovered that the process of recertification could take up to 105 days starting at the actual due date. During this whole period of time the organizations will stay on the "active" list.

53. As long as the organizations still publicly commit to apply the Privacy Shield Principles this might not lead to a gap in the protection of individuals. **However the EDPB reiterates that it is the reasonable expectation of individuals who consult the Privacy Shield list that all organizations listed as "active" have current and valid certification checked by the DoC. The EDPB is of the opinion that the change of practice to already set a new due date on the Privacy Shield list as soon as the recertification documents are submitted to the DoC does not lead to the result that only fully checked certifications are displayed as "active" on the List. The EDPB still asks the DoC to explore what can be done to avoid this situation** (especially what can be done to guarantee that there is no gap in the protection of individuals) **and in the meantime to add some explanation for concerned individuals and EU based organizations using the Privacy Shield as a transfer tool so the situation is sufficiently clear to individuals and also organizations within the EU that would like to transfer personal data to a Privacy Shield certified organization and therefore check the validity of the certification on the Privacy Shield List**.

54. During the course of the third Joint review it was also discovered that on the Privacy Shield list there were 29 Organizations listed as "active" that had a due date in 2018. **The EDPB asks the DoC to implement procedures that make sure that the "active" list of participants is always up to date and to implement checks that avoid such outdated listings.**

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC

55. In the first Joint Review report the WP 29 criticized that the **oversight of the commercial aspects of the Privacy shield mainly relied on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the **implementation** of the Privacy Shield framework **lacked sufficient oversight and supervision of compliance in practice**. Because the Privacy Shield is a program based on self-certification, it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities. The WP 29 considered that the **performance of compliance reviews** of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework and that **ex-officio investigations have to be conducted both by the DoC and the FTC/DoT** to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield.

56. The second review showed that the U.S. authorities (namely DoC and FTC) had made significant efforts to address this concern:

- On a quarterly basis the DoC conducts "false claims reviews" in order to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

  The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the "active" Privacy Shield List.

- As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.

- The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from the designated point of contact; the Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30-day period how it has addressed the concerns. If those are not resolved within the 30 days, the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT.

- The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.
- The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.

57. This year, the DoC indicated that it issued more than 670 warning letters, most of them regarding false claim participation.

58. Aside from the fact that the DoC has increased the amount of random spot checks to 30 randomly chosen organizations per month, the third Joint Review did not reveal any further developments in this direction.

59. **Therefore, while the EDPB still welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield because they remain a good starting point; the EDPB is deeply concerned that these checks still remain focused on the formalities to be complied with rather than on the substance. The EDPB urges the DoC to extend the oversight activities also to substantial elements, such as the purpose limitation principle for instance.**

60. Further to monitoring concrete compliance with all principles of the framework, **one of the areas that would need particular attention in this context remains the area of onward transfers.** The DoC has still not made use of its right to request a copy of the relevant privacy provisions of organizations contracts with their agents. **Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance to closely monitor the practical implementation of the Accountability for the Onward Transfers Principle.**

3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC

61. In last year's review the EDPB noted an increase in the FTC´s activities regarding the enforcement of the Privacy Shield. This year however, the FTC recognized that due to its lack of budget, it had to prioritize its actions with regards to the enforcement of Privacy rules.

62. While last year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification and 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield. The FTC indicated that some investigations into potential Privacy Shield violations remain ongoing, without further clarifying their scope and the exact number of cases. This year the FTC has brought 7 new cases regarding the enforcement of the Privacy Shield, still on administrative failures and not on the substance of the Privacy Shield's principles. The EDPB stresses that further controls concerning onward transfers could be led, given that the solutions put in place by the certified companies are not checked by the DoC either.

63. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers almost exclusively working only on privacy. They are supported by for example technical experts.

64. The FTC investigates Privacy Shield-related referrals (143 discovered "false claim cases" in the third year) but in most cases by the time these referrals arrive to the FTC they have been solved in the meantime so many cases fall out.

65. Concerning the Facebook settlement reached since last year's joint review, the FTC clarified that the scope of it remains outside the scope of the Privacy Shield as none of the products covered by the settlement were certified under the Safe Harbor or the Privacy Shield[21].

66. **The EDPB still welcomes any ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets the low number of cases concerning the enforcement of the Privacy Shield and that the FTC still was unable to share any more detail on its approach as this leaves the EDPB unable to have a clear insight on the concrete activities and cases, and therefore to be in a position to assess how and to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.**

3.6 Independent Recourse Mechanisms

67. The independent dispute resolution providers reported an overall increase in both the number and complexity of the complaints received under the Privacy Shield framework since the second joint review. The EDPB acknowledges that the number of complaints slightly raised and were resolved in a timely manner. However, the increase of complaints in general do not entirely compensate for the lack of proactive checks from the competent US authorities. Indeed, from the feedback collected during the Joint Review, the complaints do not seem to concern the issues of concerns underlined by the EDPB so far as they seem to mainly focus on procedural aspects.

68. In the report of the second annual joint review, the EDPB expressed its expectation to see improved and comparable reports provided by the IRM services that also explain how possible conflicts of interests are precluded. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests, and updated its guidance on Annual IRM report to include potential conflicts of interest and the description of how they avoid such situations. However, the guidance developed and standardized forms issued do not cover all aspects of the reports. In particular, the EDPB found that no standardised template format for the reports have been introduced yet on this aspect. In order to ensure full comparability, the EDPB therefore recommends the DoC to introduce a standardized template format for the Annual IRM report, which also contains explanation on how possible conflicts of interests are precluded.

3.7 HR Data

69. As already stated in the previous reports, the notion of HR data in the context of the Privacy Shield is interpreted differently within the EU and by the US authorities. Although the DoC initiated the producing of guidance regarding the processing of HR data, including through informal consultation of members of the WP 29 and of the EDPB later on, on working level in this regard, the work on this guidance was not successful yet due to the absence of convergence on the definition of the notion of HR data. Last year's review thus focused less on the definition of HR data but rather on the consequences, the different definitions within the EU and by US authorities may lead to. On the EU side, the concern is that additional protections granted by the Privacy Shield for employment data (opt-in to marketing purposes rather than opt out) would not and could not be enforced by any U.S or EU authority. The EDPB recalls that in its understanding, HR data should be protected in the same way whether they are processed by the employer or by a processor, including concerning the choice and

21 The effects of the immunity of the settlement reached however remained unclear. Indeed, this immunity would not prevent individuals to bring actions against facebook for other products, or for practices which were unknown at the time of the settlement. However, should facebook adhere to the Privacy Shield in the future for the products covered by the settlement, without changing anything from its commitments, it is still to be clarified whether the immunity derived from the settlement would cover corresponding violations of the Privacy Shield in this context for the practices covered by the settlement.

purpose limitation principles. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. **In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

70. In the report of the first annual review, the WP29 called upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.

71. As part of the second review the Commission presented the main elements of a study[22] commissioned to an independent contractor regarding the existence of automated decision-making on the basis of personal data that has been transferred from the EU to Privacy Shield certified companies in the US. While the authors of the study highlight a series of challenges for conducting this work (limited availability of experts on the topic and reservations to take part in interviews, limited relevance of answers in certain cases, opacity characterizing the data industry on such practices notably), the main conclusion that can be drawn from the study is that automated decisions (in the narrow GDPR definition of decisions having legal effects on individuals or similarly significantly affecting them) are not taken on the basis of data transferred from the EU. According to the study, such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

72. However, the study at the same time underlined that this is a fast developing area which still has to be closely monitored in the future, therefore this issue was also discussed at the third annual joint review.

73. In their reply to the questionnaire sent by the Commission in preparation to the third joint review, one trade association reported that member companies that employ automated decision-making included information about this in their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.

74. During the third joint review, the FTC confirmed that the U.S. adheres to the OECD Recommendation on AI [adopted on 22 May 2019].

75. The FTC specified that companies are not required to provide the right to know the logic involved and to request reconsideration on a non-automated basis under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy Shield). If companies do commit themselves to provide these rights, but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).

76. **Based on the findings of the third joint review, the EDPB is on the opinion that it is important that the Commission continues monitoring cases related to automated decision making and profiling and**

22 See: https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf (last accessed on 19 December 2018)

to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to challenge the decision obtaining human intervention when the decision significantly affects him or her.

4 ON THE DEROGATIONS TO THE PRIVACY SHIELD TO ALLOW ACCESS TO DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES

4.1 Introduction

77. **Since the second Joint Review, the US legal framework has not substantially changed.**

78. Consequently, some of the main points of concern that the WP29 and the EDPB expressed in their previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a reminder of the EDPB's analysis.**

79. **In addition,** this year's joint review took place at the time the "Schrems II" case, also concerning the Privacy Shield, is pending before the CJEU (the Court held the hearings on this case on 9 July 2019).

80. Also taking this background into account, specific points were discussed with the U.S. authorities during the Privacy Shield Review (*See infra*, in particular concerning PPD28, when data are collected outside the US).

4.2 Collection of data (under section 702 and under EO 12333)

81. As recalled in the previous reports, the CJEU underlined in its Schrems judgment[23] that the "*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*"[24] and ruled that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*"[25].

82. **The previous concerns expressed therefore remain relevant,** as the legal framework has not significantly changed on any of the aspects concerning the collection of data from the perspective of EU individuals (and non-US persons). Therefore, the EDPB recalls the concerns expressed in this respect in the two previous reports.

4.2.1 Collection of data for national security purposes under Section 702

83. The EDPB stresses once again the need for independent assessment on the necessity and proportionality of the definition of "targets" and of the concept of "foreign intelligence" under section 702 FISA (including in the context of the UPSTREAM program), and maintains its call for further independent assessment of the process of application of selectors in specific cases ("tasking of selectors"). It also maintains its call for further clarification in the context of the UPSTREAM program to exclude that massive and indiscriminate access to personal data of non-U.S. persons takes place.

23 Case C-362/14, 5 October 2015
24 See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.
25 See recital 94.

84. With regard to 702 FISA, it was clarified during the discussions of this year's Review that a "person" to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals would be non-U.S. persons and fulfill the applicable criteria for being targeted[26].

85. **The EDPB welcomes that the now fully functional Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency, has decided "to review the FBI's querying (searching) of data obtained pursuant to Section 702" as well as the fact that the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account. However, it regrets that PCLOB does not intend to prepare and issue an updated general report on Section 702, building on the report issued in 2014, especially given that since then section 702 was reauthorized. A general updated report would help provide an assessment of the new provisions inserted in Section 702 in the context of its reauthorization, as well as on the practice of other agencies than the FBI, in particular intelligence agencies.**

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

86. **In the context of the third Joint Review, given the disagreements between the EDPB and the US authorities as to the relevance of Executive Order 12333 for the adequacy decision, the application of Executive Order 12333 was still not further discussed.**

87. As underlined in the previous reports, the EDPB maintains the WP29 long-standing position that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal **data "on its way" to the country, for which adequacy is recognized**. The EDPB recalled this position before the CJEU[27]. During the previous Joint Reviews, the U.S. authorities underlined that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield.

88. Once again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB stresses the importance of the awaited PCLOB's reports on this text. However it understands that they are likely to remain classified, so that no further information on the concrete operation of this Executive Order and on its necessity and proportionality would become available neither to the public, nor to the Review team of the EDPB.

4.2.3 Safeguards provided in Presidential Policy Directive 28 (PPD-28)

89. The U.S. authorities confirmed once again their commitment to comply with the rules set in the Presidential Policy Directive 28 (PPD-28). The EDPB welcomes this commitment. At the same time, the EDPB stresses that the PPD-28 provides for the only safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. law do not apply. These limitations mainly concern the collection of data, as the signal intelligence activities have to be as "tailored as feasible".

90. **No new substantial discussion took place in the context of the third joint Review, concerning the interpretation and application** of the six purposes allowing for the use of data foreseen in this Directive, or relating to the amount of personal data collected by the U.S., that would allow a validation

26 For instance, this could cover for a couple using the same email address or the members of an organization using the same communication app account.

27 At the hearing organised on the 9 July 2019 in the so-called Schrems II case (C-311/18)

of the commitments and the assurances provided by U.S. authorities. In the context of this year's Joint Review, discussions mainly focused on the interpretation and application of the additional ground (situation/scenario) for bulk collection foreseen by the first sentence of footnote 5 of Section 2 PPD-28[28], which provides that "*The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection*." The U.S. authorities explained the meaning of "*signals intelligence data that is temporarily acquired to facilitate targeted collection*". The EDPB understood from these discussions that this footnote means that data may be collected in bulk - and regardless of the six purposes foreseen in Section 2 - if collected temporarily, with a view to establishing an identifier for a defined target. This would thus be an additional ground to collect data in bulk, and in this case general principles of Section 1 of PPD-28 would still apply. The EDPB regrets that the notion of "temporarily" could not be further specified, as in the EDPB's understanding, it appeared to mean that as long as the target has not been identified, bulk collection could continue.

91. The EDPB also recalls that a more detailed follow-up report on how the key terms of the PPD-28 are practically understood and applied in the different surveillance programs would be welcome, since it could provide additional information clarifying these aspects.

92. In addition, although the U.S. authorities claimed that Executive Orders and Presidential Policy Directives have "the force of law", the EDPB recalls that in the context of the previous Joint Reviews, it was also clarified that these violations of the instruments can never be - in themselves - relied upon for an action by an individual before a Court. Therefore, it would not be possible for an EU individual to directly invoke the violation of PPD-28 safeguards to bring an action before a U.S. Court.

4.3 Oversight

93. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, which the CJEU and the ECtHR have also emphasized in the respective jurisprudence.

94. Already during the two previous annual Joint Reviews, the oversight activities of several entities were presented. The EDPB considered that a **comprehensive oversight structure** is in place, composed of different elements that are in part, independent from the Intelligence Community, including the Privacy and Civil Liberty officers, the Inspector Generals, the PCLOB, the FISC and Congress, amongst others.

95. **The EDPB welcomes the appointment of the last missing members of the PCLOB. The PCLOB is now fully functioning and operational. The PCLOB also presented, for the first time, its work program, and the EDPB welcomes this step in terms of transparency from this oversight body.** As emphasized before, the EDPB considers the PCLOB, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been particularly helpful to understand the functioning of the various programs, as an independent body, an essential element of the oversight structure. The EDPB calls again for public reports to be published, including on crucial aspects of the U.S. legislation such as the three reports (one of which only is already finalized) on EO 12333, especially since the functioning of this piece of legislation could never be discussed during the joint reviews. In this context, the EDPB also regrets that, although the PCLOB indicated it would follow-up how the previous recommendations expressed in their report concerning section 702 were taken into account (see supra as well), no general updates of previous reports will be prepared, be it on Section 702 FISA or on PPD-28. Furthermore, the EDPB recalls that in the context of joint reviews organized for other EU instruments such as for PNR agreements or for the TFTP agreement, members of the Review Team are

28 Which applies only to Executive Order 12 333 and not to Section 702 FISA, which does not allow bulk collection.

given access to more information than the general public. However, in the case of the Privacy Shield joint reviews, the members of the review team only have access to the same documents as the general public. They recall that they remain ready to review additional documents and discuss additional elements under security clearance, in order to have more meaningful reviews.

4.4 Redress for EU individuals

96. As already highlighted in the previous reports, the EDPB underlines that in its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal[29]. A third-country can only be considered as providing an adequate level of protection in accordance with the GDPR, where EU individuals have access to an independent and impartial redress body, including in surveillance matters.

97. **As the U.S. government informed during this year's Joint Review that the legal framework is unchanged and no significant new case law concerning these matters needed to be considered, the EDPB recalls its position and the relevant criteria to take into account when assessing the level of adequacy are still those stemming from the jurisprudence of the CJEU and ECtHR**.

98. As repeatedly stressed in the previous reports, while the APA and FISA appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the **"standing requirement"**.

99. Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit concerning a surveillance measure on the basis of section 702 FISA or EO 12333. The EDPB will therefore continue to follow closely the evolution of these cases as they could trigger the establishment of new additional guarantees having a positive impact on the effectiveness of judicial redress offered to EU individuals before U.S. courts. However, as was confirmed during the Joint Reviews, the interpretation of the notion of "standing" in surveillance matters is evolving with cases still pending[30].

4.5 Ombudsperson mechanism

100. **In the context of the third Joint Review, the EDPB welcomed the nomination of Mr Keith Krach, on 18 January 2019, as "permanent" Ombudsperson**

101. The **Ombudsperson** mechanism aims at complementing the possibilities of redress. More critically, it might be argued that it is meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters. The WP29 therefore welcomed the establishment of the Ombudsperson, as this could constitute a significant improvement in terms of protection of the rights and freedoms of EU individuals with regards to U.S. intelligence activities. In addition, it was confirmed that the PPD-28 does not create enforceable rights for the individuals (see supra). The Ombudsperson mechanism provides the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument by asking the Ombudsperson to refer the matter to the competent authorities, which include the Inspector General, to check the internal policies of these authorities.

102. Having regard to Article 47 of the Charter of Fundamental Rights of the European Union, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high.

29 See paragraph 95
30 See in particular cases ACLU v. Clapper, and Wikimedia v. NSA.

Having analysed the jurisprudence of the ECtHR in particular, the WP29, in its Opinion of 13 April 2016, and the EDPB assessed the Ombudsperson mechanism in their opinions and in previous reports, and suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson, who can be dismissed at any time without notice, is problematic having regard to aforesaid requirements of independence and impartiality[31].This concern is also raised by the designation, as Ombudsperson, of Mr Keith Krach, given the fact that he is the Under Secretary of State for Economic Growth, Energy, and the Environment.

103. In addition, the EDPB recalls that during the first and the second Joint Reviews, as well as before the EDPB Plenary in July 2018, the previous Ombudsperson and the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The previous Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and underlined that they could escalate the issue should they be unconvinced by the outcome presented to them following the assessment of a request. These aspects were confirmed by the new Ombudsperson, who also underlined his personal commitment to only sign letters to close cases when convinced that they had been dealt with in a proper way. While the EDPB still has no reason to doubt the integrity of the new Ombudsperson, **it recalls its expectation to learn more about the powers of the Ombudsperson vis-à-vis the Intelligence Community**. This information still remains partial. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain partially classified.

104. As the first case referred to the Ombudsperson mechanism since the second Joint review was eventually declared inadmissible because it concerned data transferred outside the scope of the Privacy Shield, the case has not allowed to further discuss in detail how cases are handled under the procedures in place after the preliminary assessment of the admissibility of a case.

105. Nevertheless, the staff of the Office of the Ombudsperson explained in abstract how an admissible case would be handled. In this context, it was explained that violations of Section 702 FISA would also be reported to the FISC, which may decide to issue deficiency order to have it remedied within 30 days.

106. Questioned about his role in the Ombudsperson mechanism, the Inspector General for the Intelligence Community ("IG") confirmed that the first complaint sent to the Ombudsperson was shared with him, and that more generally in the context of requests sent by the Ombudsperson, he would, depending on the circumstances of the case, refer it to the competent intelligence agency, and that a remedy could be proposed to the ODNI. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain). He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. Nevertheless, the IG confirmed that in his report to the Ombudsperson, he could remove information from the report to the ODNI in order to protect sources and other sensitive information. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.

107. With regard to the first case under the Ombudsperson mechanism, the EDPB is committed to assess its internal processes in light of the experiences made and to adapt them, if need be.

31 See WP29 Opinion 'European Essential Guarantees', Guarantee C, referring among others to ECtHR, Zakharov.

108. In conclusion, based on the available information, the EDPB still doubts that the powers of the Ombudsperson to remedy non-compliance vis-a-vis the intelligence authorities are sufficient, as his "power" seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfill their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, the EDPB recalls that the decisions of the Ombudsperson cannot be brought to court for judicial review.Therefore, the lack of judicial review of the decisions of the Ombudsperson, and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer (failure to act) or provides an unsatisfactory reply to the complainant, still remains a concern. **As a conclusion, the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient independence, and with sufficient powers to access information and to remedy non-compliance. Thus, it cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the Charter of Fundamental Rights[32].**

4.6 Access to data for law enforcement purposes

109. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure (notably, due process) imply that data are accessed by the competent public authorities for a specific purpose and that the individual concerned is notified if her or his data have been accessed within the framework of a criminal proceeding, in the context of which they can raise objections to the collection and use of such data and have access to judicial redress.

110. However, the EDPB recalls the concerns - already expressed in the previous opinion issued by the WP29[33]- regarding the availability of effective remedies to the individuals concerned in cases where the data processed by companies is accessed by law enforcement authorities[34].

5 CONCLUSION

111. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially ex officio oversight and enforcement actions, as well as the appointments of the last missing members of the PCLOB and of a permanent Ombudsperson.**

112. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

113. **As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and** the application of the principles when it comes to **processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations.** In addition, the EDPB recalls the **remaining issues** with respect to certain

32 A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.
33 See WP 238.
34 Concerning access to data for law enforcement purposes, we also pointed out, supra, at Section 2.1 of this Report/Conclusions, to the possible access (querying) by law enforcement authorities to data acquired under Section 702 FISA.

elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.

114. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets** that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. **The EDPB would be very interested on an additional report on PPD-28 to follow up on the first report** including an assessment of how the safeguards of PPD-28 are applied Finally, the EDPB underlines the importance of reports on Executive Order 12 333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. **The EDPB recalls that the security cleared experts of the EDPB remain ready to review additional documents and discuss additional classified elements**, in order to have **more meaningful reviews**, following the example of PNRs or TFTP reviews.

115. **On the Ombudsperson mechanism**, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, **the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights**.

116. Finally, the EDPB recalls that the **same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending** before it.

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW

Factual findings of the third annual joint review of the EU-US Privacy Shield

GENERAL INFORMATION

1. The U.S. Delegation was composed of high level representatives.

2. As of now, the Privacy Shield List contains around 4984[35] organizations, 509[36] are on the "Inactive" List either because they have voluntarily withdrawn from the program (39 in the last year), not submitted their recertification in a timely manner or because their recertification has been initiated but not completed in a timely manner. There was no case where an organization was removed from the List because it persistently failed to comply.

3. Of the participating Organizations 70 - 75% are small and medium size organizations with less than 250 employees. 96% of the participating organizations certified for non-HR data transfers, 33% for HR transfers. The main businesses certifying are: Information and Communications Technology, Business and Professional Services, Media and Entertainment, and Education.

1 ON COMMERCIAL ASPECTS

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program

4. The DoCs method and scope of checks in the initial review of a certification and the recertification has not changed substantially since the last review. The DoC reviews all self-certifications (first time applicants as well as recertification submissions) for:

    1. Registration with IRM
    2. Payment of Annex I Arbitral Fund Contribution
    3. Compliance with supplemental principle 6
    4. Completion and consistency of certification information
    5. Privacy notices

5. DoC has rejected 9 first time certifications in the last year because the applicants were not eligible to participate in the Privacy Shield because they were not under the jurisdiction of FTC or DoT (5 non-U.S., 4 non-profit organizations).

6. Also, there were no significant changes reported as regards the depth of the analysis the DoC performs: the DoC checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR). It does not check if the data transferred is necessary and proportionate to the purpose for instance because they consider that the Privacy Shield does not go into this level of detail, nor do they check in substance the compliance with other principles.

[35] See https://www.privacyshield.gov/list on 24 September 2019
[36] See https://www.privacyshield.gov/inactive on 24 September 2019

7. In order to address the concern expressed by the WP29 regarding the duty of the certifying organization to publish their privacy policy referring to the Privacy Shield certification before the DoC has completed the exercise of checking and listing the organization, the DoC has changed the procedure.

8. The DoC:

   - Prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification
   - Requires an applicant to submit a draft privacy policy for review
   - Directs an applicant to remove any premature references

9. As the practical experience with the certification process increases, the DoC still uses the same guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links to their privacy policies so individuals could more easily exercise their rights, they ask for more than one point of contact within the organization to make sure messages from the DoC are received.

10. In addition to the 2-weeks-notice of the upcoming deadline to recertify organizations already sent out before the second annual review, the DoC now also sends a reminder one month and one week before the recertification is due.

11. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date. The DoC stated in the third annual review that organizations that fail to do so within 30 days after the due date are "automatically" moved to the "inactive" list.

12. Since August 2019 the DoC has changed their practice and changes the "Next Certification Due Date" on the Privacy Shield list as soon as any documents for recertification arrive at the DoC.

13. In the course of the 3rd annual review the participating representatives of the EDPB submitted a list of organizations whose recertification due date lay in the past. For 29 of those organizations the due date dated back to 2018. Checks of that list performed on September 25, 2019 led to the result that the DoC moved 87 of those organizations to the "inactive" list. Two organizations disappeared from the whole list. 213 remained on the "active" list.

14. As regards guidance, the DoC has published new guidance material for organizations to address questions around Brexit. The review team is not aware that this guidance was created in cooperation with EU SAs or the EDPB.

1.2 Oversight and supervision of compliance with the principles - Activities by the DoC

15. The DoC still identifies on a quarterly basis organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

16. If organizations do submit the paperwork necessary for recertification, the DoC foresees a timeslot of 45 days in which the recertification should be finished. If this is not the case and at least further action to complete the process is not taken by the organization, the DoC sends it a warning letter explaining that if the required action is not taken within a period of another 30 days, the organization will be removed to the "inactive" list and referred to the FTC or DoC.

17. As foreseen in the Privacy Shield text, the DoC still performs random web searches for false claims of participation in the program.

18. In the last year the DoC referred 143 discovered false claims cases to the FTC.

19. After the DoC has performed a sweep of 100 randomly chosen organizations in the second year of the Privacy Shield, it has now started in April 2019 to perform 30 of those checks each month. The focus of the sweep is the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. In case those checks result in conspicuities (about 20% of the cases) the organizations receive more in-depth compliance questionnaires from the DoC. Through this procedure minor or more significant peculiarities may appear (for example: no response from designated point of contact; privacy policy was no longer accessible online; missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter (3 in this year) requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT. It was confirmed that even if the case was resolved within the 30 days the DoC could refer it to the FTC.

20. In total the DoC has sent out 669 warning letters to participants of the Privacy Shield since October, and 1 100 were sent in total since the beginning of the programme.

21. The DoC still follows the media and does keyword searches to identify possible breaches of the Privacy Shield commitments.

22. The DoC also still performs regular checks for broken links to the privacy policy on the Privacy Shield list.

23. The DoC has still not made use of its right to request a copy of the relevant privacy provisions of an organizations contract with an agent.

24. Besides the Privacy Shield News and Events section on the website of the DoC that covers several kinds of news and also FTC decisions related to privacy in general but there is no dedicated link to Privacy Shield cases of the FTC as described in the text of the Privacy Shield.

25. In relation to the DoC's work in order to ensure that all organizations recertify and finish their work on time but also for the web searches for false claims and any other aspects of their work the DoC mentioned that it works on improving their technical possibilities.

26. The DoC has in various contexts throughout the review also uttered its wish to establish a closer cooperation between the DoC and the EDSA/ representatives of European Supervisory Authorities (for example on outreach and education, possibilities of more substantial checks).

27. The US CIB announced that they would stop managing the fund set up (to cover the costs of the EU informal panel responsible to take care of complaints submitted mostly from employees whose data have been transferred under the Shield) in accordance with the Privacy Shield in 2020. EU Commission and DPAs were approached to help finding a solution but declined any responsibility in managing it.

28. **European Commission and EDPB representatives' presentations** The European Commission, EDPB Chair and representatives gave a short presentation on the updates about the work done on the European Union side.

1.3 Independent Recourse Mechanism (IRM)

29. The DoC reported that it has developed guidance to the IRMs in order to avoid possible conflicts of interests.

30. One IRM explained once again that such a conflict of interest would be avoided by separating the teams providing IRM services and those verifying ex officio compliance with the Privacy Shield framework, both in terms of tasks and staff. Regarding the management of such potential conflicts between the two teams, it reported on having its own department that monitors these conflicts and has not had identified any so far.

31. Potential conflicts of interest must be included in the annual reports of the IRMs, but neither this aspect of the report was standardized nor any standardised template format for the reports have not been introduced yet.

32. In total, the IRMs received 48 complaints under the Privacy Shield framework and reported an overall increase in both the number and complexity of the complaints.

33. However, the IRMs reported that only one-third of the received complaints were eligible under the Privacy Shield. The other complaints were primarily regarding U.S. companies that were not self-certified under the Privacy Shield framework.

34. The majority of the complaints received were related to requests from individuals regarding a change or removal of their personal data, an unsubscription from the organizations services, the disabling of accounts and the contact with a representative from the applicable organization.

35. Another IRM reported that three complaints were successfully resolved, which related to the access principle as well as the improper handling of the notice principle.

1.4 Arbitral Panel

36. The fee that according to the Privacy Shield text is collected from the certified organizations annually is still being collected only once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to more than 5 million $.

37. Regarding the arbitral panel procedure, two requests were submitted since the second annual review. Both requests were dismissed as one failed to comply with the steps needed to invoke such an arbitral panel procedure and the other one did not relate to a company that was a Privacy Shield participant.

1.5 Oversight and supervision of compliance with the principles - Activities by the FTC

38. The FTC representative answered the questions of the Commission and the EDPB along the following 3 main categories:

1.5.1 Concerning the status of the Privacy Shield enforcement in general

39. 7 Privacy Shield cases were handled since the last review, to look more into substantive violations of the framework.

40. Two cases concerned the supplemental principle 6 (on the obligation to continue to apply the Privacy Shield to the data collected after withdrawal from the programme). The FTC also focused on supplemental principle 7 (obligation to verify or certify that the company has assessed its compliance with the Privacy Shield).

41. The FTC also performed *ex officio* reviews: 1 case this year, where the company did not comply with this principle 7 (and thus probably with others). The representative of the FTC announced more cases on the Privacy Shield to come.

42. Following a question from the Commission, the FTC answered that it did not focus only on the formal respect of the Privacy Shield, but also on the substance.

1.5.2 On the Facebook case which led to the recent settlement with the FTC (follow-up of the discussions in the second Joint Review and update on this case)

43. Although the representative of the FTC underlined that they could not share much details as the findings have not been made public, it was indicated that eventually the investigation focused on products for which Facebook did not certify under the Privacy Shield (Facebook only certified for two new products, Workplace premium and Ads Measurement). Thus, contrary to what was expected during the second review of the Privacy Shield, the settlement reached does not have a direct link with the Privacy Shield.

44. The FTC clarified that as an effect of the settlement and of the immunity deriving from it, in the future it could only take action against Facebook concerning violations which were unknown at the time of the settlement (for instance, a new complaint on a new subject or concerning a different service). This means that if Facebook adhered to the Shield for these products without any further change, the FTC would probably not be in a position to act and that existing complaints on the aspects covered by the settlement will not be handled further.

45. Concerning the possibility for the FTC to contemplate a repetitive practice, for instance in terms of the exercise of rights of data subjects, as a persistent failure to comply, the DoC indicated that it is a possibility if an organization regularly fails to comply and it is no longer possible to assume that it is limited to an individual case.

46. Questioned about the settlements in general, the FTC indicated that it had to offer the company the opportunity to settle in all privacy cases, when the FTC is ready to open a case before the court. The FTC could refuse to settle, for instance when they have civil penalty. However the FTC would not impose a fine that would make the company go bankrupt. When calculating the amount of money for the settlement, the FTC would have to take into account how much the company earned from its practice and add the amount of the fine, according to the principle that a company shall not profit from its misconduct.

47. For each civil penalty, the FTC underlined that it was required to look at multipliers: degree of guilt, the ability to pay, deterrence and harm to consumers.

48. Concerning the interactions of the FTC with the DOJ in the context of settlements, the FTC stressed that it does not have the power to impose a civil penalty on its own and that in such situation they would have to refer the case to the DOJ, which then has 45 days to either take the case or let the FTC take it back. In case the DOJ takes the case on behalf of the State, the FTC underlined that they usually follow the recommendations made by the FTC.

1.5.3 On the general developments in US privacy law that may affect the Privacy Shield and on the resources of the FTC

49. The representative of the FTC underlined that the Federal Trade Commission's policy is to be aggressive towards companies within the boundaries of the powers they have (i.e., in cases for which the FTC is able to impose civil penalties).

50. Several cases were initiated or finalized this year.

51. The FTC is also continuing its hearing process to improve their orders. This process already resulted in the additional requirement to companies to have their assessor for outside compliance reviews approved. These assessors are also required to provide the FTC with all the documents in their possession.

52. Nevertheless, the FTC stressed its lack of effective means to perform its duties and missions (lack of resources, restricted competence and powers, e.g. with respect to non-profit organisations, etc). In this regard, it was underlined that without further resources, the FTC would not be in a position to process more than 7/8 cases regarding the enforcement of the Privacy Shield per year (although the duration of investigations vary from one case to another). The FTC is continuously advocating for a stronger law on first-time violations, the ability to reach non-profit entities, and for more resources.

53. Questioned on its investigatory powers, the FTC confirmed that they could have access to source codes with the issuance of subpoenas. Regarding the criteria used to prioritize their investigations, the FTC indicated that they try to maximize the yield of their resources. They do not plan "fishing expeditions" in advance, but prefer to collect information from open sources that may make a case. It sets it priority on cases regarding sensitive information (credit, finance, health, children information). The FTC stressed that, in principle, they are not an examination agency. Consequently, they could but do not usually investigate on-site but rather use documentation and interrogatories.

1.6 Oversight and supervision of compliance with the principles - Activities by the DoT

54. The DoT is in charge of the supervision of data processing related to air transportation, which includes two main entities: airline companies, and ticket agents. To date, no airline company is participating in the Privacy Shield, and only very few ticket agents.

55. Because the situation of DoT is very similar to that of the FTC, it looks closely at FTC's practice and case law. The DoT has not received any Privacy Shield related complaints so far.

1.7 Onward Transfers

56. The representatives of DoC underlined that FAQs on how to comply with the Accountability for Onward Transfers Principle, published before the second review, are available on the Privacy Shield website. They contacted law firms, consultancy agencies and other stakeholders to seek more information about their experiences and expectations regarding this issue. These organizations indicated that the negotiation of the clauses on onward transfers are usually part of a wider, general negotiation, in which not only the Privacy Shield principles, but US states law also has to be considered (eg. existing state law requirements on data breach). According to the information gathered as a result of this outreach, the organizations found the FAQs helpful.

57. The DoC does not get specific questions from organization on onward transfers during the certification and re-certification process, applicants usually have more general questions on the interpretation of the Privacy Shield Principles.

58. Questioned about DoC's possibility to request a summary or copy of the contract used by an applicant to comply with the principle on onward transfers, the representatives indicated that they did not make use of this possibility so far. The DoC also indicated that it is not part of the compliance questionnaire and the sweep checks to verify specifically these contracts, and the compliance with the Accountability for Onward Transfers Principle.

1.8 Automated decision-making/Profiling

59. The FTC confirmed that the US adheres to the OECD Recommendation on AI [adopted on 22 May 2019].

60. In their reply to the questionnaire from the review team, one trade association reported that member companies that employ automated decision-making included information about their policies and maintain mechanisms to allow consumers to exercise control, such as the ability to contest an automated decision and seek human review.

61. The FTC specified that companies are not required to provide such rights under the Privacy Shield (and therefore, to include a reference in this regard in the privacy policy submitted pursuant to the Privacy shield). If companies commit themselves to provide these rights but then, contrary to this commitment, they do not provide them, this will constitute a misrepresentation, against which the FTC can take enforcement action.

62. In the area of consumer credit, the FTC referred to the Fair Credit Reporting Act (FCRA).

1.9 HR Data

63. In the course of the review the EDPB review team was approached by the DoC to further discuss this issue. The main topic was the possible loss of European oversight for European employees and their expectation in terms of rights (notice and choice). On the other hand for certain service providers, the DoC underlined that it might be difficult to even know if they are processing employee data. Arguments and possible solutions were exchanged. The DoC took note of those and will contemplate on possible ways forward. There is no concrete outcome of the discussions yet.

1.10 US domestic privacy update: NIST Framework

64. The National Institute of Standards and Technology (NIST) presented the last version of its "Privacy Framework" (preliminary draft, 6 September 2019). The Privacy Framework, customizable by companies, aims at providing guidance to companies on how to reach a certain level of data protection (the process), without pre-setting the level to be reached ("desired privacy outcomes").

2 ON GOVERNMENT ACCESS TO PERSONAL DATA: RELEVANT DEVELOPMENTS IN THE U.S. LEGAL FRAMEWORK AND TRENDS

65. Legal framework has not changed substantially.

2.1 Ombudsperson mechanism

66. During the review, Keith Krach presented himself as the new Under Secretary for Economic Growth, Energy, and the Environment of the U.S. Department of State, and the Privacy Shield Ombudsperson. He stressed that the Ombudsperson mechanism needs to provide an effective, empowered channel of review for EU individuals.

67. He also confirmed to be independent from the Intelligence Community (IC), and stressed, as his predecessors did during the first and second reviews, that he will not sign his name to a letter if he would have any remaining doubts on the completion of appropriate redress.

68. The Ombudsperson's staff then reported that the only request received under the Ombudsperson mechanism was in agreement with the EU Centralized Body found to be deficient.

69. Referring to a hypothetical case, the staff then presented in general terms the procedures and powers of the Ombudsperson, stressing that the Ombudsperson would have access to all information he needs to perform its duties and that all incidents of non-compliance would have to be remedied, including the purging of data. It was also provided that violations of section 702 FISA would be reported to the FISA Court.

70. No further specific information about how the Ombudsperson would cooperate with the IC were shared, as the Ombudsperson reported that those procedures continue to be classified.

2.2 Inspector General (IG)

71. The Inspector General of the IC gave an overview of how IGs are set up and operate within the U.S. government and the U.S. legal system. He stressed that IG's are independent from the bodies they oversee, and that they are empowered by law to review and investigate any abuse of power.

72. The IG reported that the request which was made under the Ombudsperson mechanism (and found to be deficient) was also examined by the office of the IG.

73. The IG confirmed that the office could take up any hint of an abuse of power, also on its own initiative. However, the IG only investigates concrete cases and does not review policy.

74. During the last year, the IG office has not investigated any matter related to the Privacy Shield.

75. Questioned about how the office of the IG would handle an Ombudsperson request, the IG explained that it would depend on the case, but that he may refer to an agency, and that a remedy may be proposed to the ODNI. He added that Congress would also be informed about recommendations and about cases where the recommendation is not followed through.

76. Further, the IG explained that the Ombudsperson would also be informed of the findings and recommendations to the ODNI necessary for the Ombudsperson to perform his duties. In order to protect sources and other sensitive information, in the report to the Ombudsperson, the IG may remove information from the report to the ODNI. As a consequence, the information shared with the Ombudsperson may not necessarily be identical to the information shared with the ODNI.

77. Finally, the IG clarified that his resources are not decided upon by the Government, but by Congress.

2.3 PCLOB

78. The summer before the third annual review, the Senate confirmed the last two members of the PCLOB. The Chair of the PCLOB underlined that the PCLOB is thus now fully staffed for the first time since 2016.

79. The staff has also doubled since the last review, and 7 new projects have been launched. Overall, the PCLOB is now working on 10 projects and also strengthened its knowledge in terms of technology.

80. For the first time, the PCLOB released an agenda of their current projects, which it will update every six months. The PCLOB also published strategic goals for the next three years, among them technology is identified to be the key factor for privacy.

81. The PCLOB representatives recalled the history of the agency and its functioning.

82. Regarding the current projects, the Chair underlined that the Board is currently working on the following issues:

    - Regarding NSA's collection of detailed call records under the USA Freedom Act. The report is expected to be finalized later this year.

- Regarding facial recognition in airports, work has started recently.
- Regarding the terrorist watchlist, a project is ongoing as well, yet without any forecast date. It was however underlined that the mere fact of working on a subject already sends a signal.
- Regarding EO 12 333, work is still ongoing:
    a. 3 deep-dive reviews were organized on this subject, 2 of those related to the CIA (1 of them is finalized and transmitted to the Congress), 1 to the NSA (on XKeyscore).
    b. The PCLOB is also providing advice on a range of guidelines on EO 12 333 for internal use.
    c. The PCLOB Chair indicated that they hope some work will be completed and made available in a relative near future.

83. Regarding the calendar of work concerning EO 12 333, the Chair indicated that each deep-dive review can be finalized independently from the others, and be declassified separately. However, the Chair of the PCLOB underlined that in spite of their strong policy towards the broadest dissemination of their works, it was unlikely that these reports would ever be (fully) declassified.

84. Regarding Section 215 and whether their report will be issued by the end this year, the Chair of the PCLOB confirmed that they hope to deliver it in sufficient time, so that it will be available to the Congress in the context of the possible re-authorization of this section.

85. When questioned on whether the PCLOB's report on Section 702 could and would be updated, the Chair of the PCLOB indicated that FBI's access and use of the data would partially be reviewed, but that the PCLOB did not intend to update the whole report.

86. Regarding the mandates the PCLOB gives itself and its work program, the Chair of the PCLOB indicated that the PCLOB has a holistic approach and that its reports focus on collection, but also look at storage, use of data, compliance mechanisms, as well as sharing and dissemination. It was also underlined that the PCLOB's focus evolves where the practice goes, and needs to migrate to those, even when they are not yet known to the public.

2.4 ODNI and Department of Justice presentation and Q/A on government access to personal data: relevant developments in the U.S. legal framework and trends

87. The Chief Privacy Officer of the ODNI confirmed again that the function of his office was to advise on the policies regarding civil liberties and privacy, according to the statues, and that the officers also have the power to conduct investigations, which includes to have access to all the materials and records needed.

88. When performing their missions, they are bound by statutes which govern their actions, by Executive orders, Attorney general's guidelines, Presidential Directives, and orders of courts. This office also provides the public with new interpretations issued by the FISC (either along with the decision or with a summary if the decision itself cannot be provided).

89. The Chief Privacy Officer of the ODNI reported that no major changes took place since the last review. He confirmed that PPD 28 remains in full force and effect.

90. In this regard, he underlined that PPD 28 demonstrates a strong preference to conduct targeted surveillance (as tailored as feasible) rather than bulk, which is, in principle, allowed only for six purposes.

91. He reaffirmed that bulk collection is neither generalised, nor mass collection, and that "bulk collection" is usually a choice, for instance to identify a target.

92. In view of a question raised by the CJEU during the hearing on the Schrems II case, in particular on footnote 5 of PPD 28, after extensive and detailed exchanges, the following elements were clarified:

    - This footnote is not applicable to Section 702 as it is not a bulk collection program (since it is based on the use of selectors). Nevertheless, sections 1, 3 and 4 of PPD 28 apply.

    - This footnote applies to EO 12 333, for instance.

    - This footnote would mean that in addition to the six purposes foreseen under PPD 28 for bulk collection, PPD 28 allows (through this footnote) an additional situation where bulk collection can take place: when bulk collection is temporary, in order to identify a target. In this case, it appears to be possible to derogate from the six other purposes foreseen under PPD 28 to undertake a bulk collection of data, but only temporarily, for another authorized purpose of collection, and in this case, Section 1 of PPD 28 would still apply.

    - Questioned on what "temporary" would mean, the answer was not very clear. It seems that, as soon as the collected data has been processed to help identify the target, useless data is no longer useful is deleted.

93. Concerning targets and selectors under Section 702, the Chief Privacy Officer of the ODNI recalled that the distinction between a selector and a target is important: the target should be a "person", while a "selector" is any communication identifier (e.g., email address, phone number, etc.) allowing to isolate the person's communication data from the bulk. However, questioned on whether a person should necessarily be only one single individual, he acknowledged that in some cases a person could be a group comprising more than one individual (e.g., the users of an email account), provided the size of the group remains limited and that any member of the group needs to have a link with the foreign intelligence at stake and to be a non-US person.

94. The way a person is selected is through the tasking of a selector, which is documented both for approval and oversight.

95. It was stressed that each selector has to be an account used by a person and that it cannot be the name of a person. It has to be a communication account identifier, thus communication always has to be from or to the selector. It was also confirmed that these safeguards related to the tasking of selectors only apply within the framework of Section 702.

96. Questioned on the time limit for which a selector is tasked, it was underlined that a selector is tasked "for as long as it brings back foreign intelligence". Regular checks would thus be performed to confirm that is still useful and necessary.

97. As regards to PRISM and UPSTREAM collection and the filtering of communications, no additional information was presented during this review.

98. At the time of targeting, the NSA shall provide a written explanation to allow for an *ex ante* review in the IC before tasking the selector, as well as a post review by the DoJ. It was recalled that in case of an acknowledged incident, collection stops, the underlying information has to be purged, and, if any reports were based on that information, these reports must be recalled (this is a standard procedure for reports in this domain).

99. In case of an incident, the office of the Privacy Officer would also have to look at the context in which it occurred and to report non-compliance to the FISC (in the context of section 702), with a description of the scope of the incident and of reasons why it happened. The Court then would follow-up on these reports, for instance by determining, in the annual certification process, whether those compliance incidents effectively rendered certification inadequate. It could also issue a deficiency order to have it remedied within 30 days. In addition, quarterly reports on incidents are also sent to the FISC.

100. In addition, the Chief Privacy Officer of the ODNI stressed that semi-annual reports of compliance incidents for the Congress are declassified to the extent allowed and made available on IC on the record, by the DoJ. These reports also show the trends of non-compliance and comments, which provide more useful information than the statistics (see the last one of March 2019).

101. Brief updates were also provided on cases introduced or ruled since the last review concerning FISA §1806 (two cases of the 9th Circuit - Jewel and Fazaga), as well as FOIA (ACLU v. NSA before the appellate court and the following cases, as well as Food marketing Institute v. Argus Leader Media from the Supreme Court).

102. Concerning the Wikimedia case, the DoJ stressed that the first instance considered that the complainants lacked standing, but this judgement was overturned by the appellate court. The case is still pending, while another case was ruled and dismissed on substance, but is being appealed too.

103. Concerning Section 501, for which the Administration is seeking reauthorization of this authority, it was recalled that the NSA is not using it any longer, because the information were too narrow and thus not sufficiently useful.

104. Questioned on how the additional safeguards afforded to the data of EU residents transferred to the US through the Privacy Shield would be reflected in executive agreements concluded between the US and another third country in the context of the Cloud Act, the DOJ indicated that it could not answer this question yet.

LIST OF ABBREVIATIONS

DoC: Department of Commerce

FTC: Federal Trade Commission

IG: Inspector General

APA: Administrative Procedure Act

FISA: Foreign Intelligence Surveillance Act

FISC: Foreign Intelligence Surveillance Court

PCLOB: Privacy and Civil Liberties Oversight Board

PPD-28: Presidential Policy Directive n°28

EO 12 333: Executive Order 12 333

ODNI: Office of the Director of National Intelligence