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

Adopted on 22 January 2019

Table of contents

1 Executive summary 4

1.1 Introduction 4

1.2 On the commercial aspects of the Privacy Shield 4

1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield 6

1.4 Conclusion 7

2 Introduction 8

3 On the commercial aspects of the Privacy Shield 9

3.1 Guidance for the companies adhering to the Privacy Shield 9

3.2 Clear and easily available information for EU individuals 10

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism 10

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC 12

3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC 13

3.6 Independent Recourse Mechanisms 13

3.7 HR Data 14

3.8 Automated-decision making/Profiling 14

4 On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes 16

4.1 Introduction 16

4.2 Collection of data (under section 702 and under EO 12333) 16

4.2.1 Collection of data for national security purposes under Section 702 16

4.2.2 Collection of data for national security purposes under Executive Order 12333 17

4.3 Oversight 17

4.4 Redress for EU individuals 18

4.5 Ombudsperson mechanism 19

4.6 Access to data for law enforcement purposes 20

5 Conclusion 20

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW ... 22

General Information 22

1 On commercial aspects 22

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program 22

1.2 Oversight and supervision of compliance with the principles - Activities by the DoC 23

1.3 Oversight and supervision of compliance with the principles - Activities by the FTC 24

1.4 Oversight and supervision of compliance with the principles - Activities by the DoT 25
1.5 Guidance for the companies adhering to the Privacy Shield 25
1.6 IRM 25
1.7 Arbitral Panel 25
1.8 Automated Decision Making 25
1.9 HR Data 26
2 On government access to personal data: relevant developments in the U.S. legal framework and trends 27
2.1 Reauthorisation of 702 FISA 27
2.2 PPD-28 27
2.3 The Ombudsperson mechanism and the EU individual complaint handling body 27
2.4 PCLOB 28
2.5 Inspector General (IG) of the ODNI 28
2.6 Redress 28
2.7 Additional information on access to data by law enforcement authorities 29

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, **seven representatives of the EDPB participated in the second joint review conducted by the European Commission, on October 18 and 19 of 2018** in Brussels 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, in particular opinion 1/2016, and in its report following the first 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 citizens**, 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 second joint review on December 19, 2018.

4. **The EDPB's main findings concerning this second 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 second annual review showed that **many of the WP 29's findings of the first annual review regarding the commercial aspects have been taken into account by the US authorities**. The EDPB acknowledges that on the commercial aspects significant progress has been made especially with regards to the following aspects.

6. The **DoC has adapted the initial certification process** in a way that the inconsistencies between the Privacy Shield List and the representations made by the organizations regarding their participation in the Privacy Shield program on their websites are now avoided as far as the initial certification process is concerned.

7. The **DoC as well as the FTC have started to also take ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield.

[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.

8. The **DoC has issued further guidance for the EU individuals** in order to facilitate their understanding of the Privacy Shield and the exercise of their rights. The **DoC has also started to issue further guidance for the U.S. Businesses** in order to clarify the requirements of the Privacy Shield. The EDPB still expects this guidance will provide the necessary clarifications to facilitate the proper application, and where necessary will be adjusted.

9. **However, one of the main concerns already expressed by the WP29 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 could not be fully assessed during the review, since the FTC was not able to share substantial information on the subject matter of the new ex officio enforcement actions taken. **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**. The Privacy Shield presents in its Annex 1 "the clarification that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing" as an enhancement of the Privacy Shield. This is only one example for many substantial requirements set out by the Privacy Shield whose correct application has to be ascertained through sufficient oversight and enforcement action by the competent U.S. authorities.

10. **Another issue where the EDPB sees further need to work on concern the area of 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.

11. **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 do not lead to gaps in the protection of EU data subjects.

12. **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.

13. 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 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

14. The EDPB **welcomes the appointments of three new members of the Privacy and Civil Liberties Oversight Board (PCLOB), including its Chair, enabling it to reach the quorum**. It hopes that the two remaining positions will also be filled, which are important to respect the requirement concerning the bipartisanism of the members. The PCLOB is thus in a position again to prepare and issue reports.

15. The EDPB also welcomes the fact that the US authorities have published the report on Presidential Policy Directive 28 (PPD-28), in a redacted form, which mainly clarifies that the PPD-28 is applied by all agencies of the Intelligence Community, and it acknowledges the efforts made by the U.S. government by publishing a number of important documents, for example, decisions by the Foreign Intelligence Surveillance Court (FISA Court), in part by declassification, and the setting up of a new website.

16. Despite these developments, **some of the main points of concern, already expressed by the WP29 in this area in its previous report, still have to be fully resolved**.

17. More specifically, the **collection and access of personal data for national security purposes** under both Section 702 of FISA and Executive Order 12333 still remains an important issue for the EDPB, **especially with regards to massive and indiscriminate access** (on this issue, see in particular the statement of the WP29 on the decision of the European Commission on the EU-U.S. Privacy Shield of 26 July 2016[2]).

18. In this respect, **the EDPB can only encourage the PCLOB to issue further reports**, on PPD-28 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 follow-up report on Section 702 FISA. The EDPB recalls that the WP29 considered a report on Section 702 important for assessing 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**), 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.

19. **The EDPB regrets that the reauthorization of Section 702 FISA did not lead to the introduction of any new guarantees for EU individuals**. The EDPB recalls that, in its report following the first annual Joint Review in 2017, the WP29 considered that instead of generally authorizing 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.

20. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB would welcome if the PCLOB finalized and issued its awaited report on EO 12 333 to provide information on the concrete operation of this Executive Order and on its necessity and proportionality.

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

[2] https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

22. 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. In any case, a permanent Ombudsperson **is still to be appointed**.

23. The exact powers of the Ombudsperson also 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 powers of the Ombudsperson 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, and also underlines that the Ombudsperson is not in a position to bring a matter before the court.

24. 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

25. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions**, as well as the efforts made by the U.S Government by publishing a number of important documents and **the appointment of a new Chair as well as of two new members of the PCLOB, meaning that the PCLOB has reached the required quorum for its functioning**. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**.

26. **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 processors, as well as the recertification process**. 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.

27. As regards the **collection of data by public authorities, the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.

28. **On the Ombudsperson mechanism**, the EDPB is **still awaiting the appointment of a permanent independent Ombudsperson**. Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not 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**.

29. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending** before the Court.

2 INTRODUCTION

30. On 6 October 2015[3], 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.

31. On the 13 April 2016, the Working Party 29 issued an opinion[4] on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document[5] on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

32. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision[6].

33. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision[7] ("Privacy Shield"). 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[8]. 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.

34. As also foreseen in recital 147, *"participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party"*.

35. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017[9].

36. The second Joint Review of the Privacy Shield took place on the 18 and 19 October 2018 in Brussels. In addition to the Chair of the EDPB who gave an introductory speech, seven representatives of the EDPB, a Commissioner as well as experts at staff level, were designated to be part of the Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities and companies.

[3] Case C-362/14
[4] WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
[5] WP 237 https: //ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
[6] EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf
[7] 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.
[8] See recitals 145-149 and Article 4(4) of the decision.
[9] WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

37. In advance to the Joint Review, the Commission sent questionnaires to US companies adhering to the Privacy Shield 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.

38. The new factual elements presented by the US authorities and companies 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 16 November.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

39. 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.

40. 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[10] and the notion of Processor**[11] and published it on its website.

41. The EDPB welcomes the issuance of these guiding documents that have been also highly demanded by participating organizations. This guidance should lead to the clarifications necessary to facilitate the proper application of the Privacy Shield Principles. In order to achieve this goal, the guidance concerning processors may further specify the application of the principles when it comes to processors ("agents")[12].

42. Regarding the usability of the European Commission's Standard contractual clauses in the context of onward transfers further work is required since the available clauses are designed only for transfers

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

[11] https://www.privacyshield.gov/article?id=Processing-FAQs (last accessed on 18 December 2018)

[12] 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.

from EU territory. In this context the EDPB calls upon the European Commission to also address this issue in the course of aligning the SCC with GDPR.

43. The EDPB regards the issuance of further guidance as a good start and expects that in the future there will be more guidance as to other key elements such as 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), and with respect to the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, 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 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"[13] 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[14] 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. It remains to be seen if the Information given to the EU individuals both by the EU Supervisory Authorities and the DoC lead to the effect that more individuals are able to exercise their rights regarding the Privacy Shield properly.

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

46. Also in the certification process, the EDPB notes improvements:

47. The DoC 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
3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
4. Completion and consistency of certification information

[13] See: https://www.privacyshield.gov/Individuals-in-Europe (last accessed on 27 November 2018)
[14] See: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq (last accessed on 14 December 2018)

5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)

48. In order to prevent organizations from naming non-U.S subsidiaries as entities covered by their certification the DoC has produced more internal guidance for the review of applications regarding the identification of foreign entities.

49. Also, the DoC 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).

50. The DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled. This appears to be an indication 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.

51. However, on the basis of the information given by the US authorities during the joint review, so far those checks do not go into the substance of the principles. The DoC for example does not check if the data transferred to an organization in the US acting as a controller is necessary and proportionate to the purpose, arguing that the Privacy Shield does not provide for checks with this level of detail. 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.

52. As regards criticism on the procedure, which used to require US organizations to publish their Privacy Policy (with references to the Privacy Shield) before the checks of the DoC were finalized and the organization was put on the list of Privacy Shield active participants, the DoC has changed its procedure. The Doc now prohibits a first-time applicant from making public representations about participation until the PS 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.

53. As a result, **the concerns of the WP 29 regarding the inconsistencies between the Privacy Shield List and the representations made by the organizations on their websites seem to have now been resolved as far as the initial certification process is concerned**.

54. **Regarding the re-certification process**, the second annual review revealed that due to the established procedures 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. This leads to confusion.

55. 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 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**.

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

56. In last year's 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.

57. This year's review showed that the U.S. authorities (namely DoC and FTC) have 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.

58. **The EDPB welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield. They are a good starting point; however, so far these checks remain focused on the formalities to be complied rather than on the substance.**

59. 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. So far the DoC has 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

60. Since last year's review the FTC also increased their activities regarding the enforcement of the Privacy Shield.

61. 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.

62. This 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.

63. The FTC investigates Privacy Shield-related referrals (about around 100 referrals, 8 of them being public) 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.

64. As an experiment, the FTC has started to send out Civil Investigation Demands (CIDs) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.

65. **The EDPB welcomes the ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets that the FTC 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

66. In order to make the reports provided by the various companies providing IRM services on an annual basis more useful the DoC gave out guidance to the IRM services in order to harmonize their reports. This guidance also highlights the possible conflicts of interest within companies providing both ex officio compliance and IRM services to the same organization and asks to describe the measures taken

to avoid such conflict of interests in the annual report. **The EDPB expects to see improved and comparable reports provided by the IRM services in the next annual review, that also explain how possible conflicts of interests are precluded.**

3.7 HR Data

67. As already stated by the WP 29 in last year's report, 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 on working level in this regard, the work on this guidance was not successful due to the absence of convergence on the definition of the notion of HR data. This 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 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 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 do not lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

68. In last year's report, 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.

69. As part of the second review the COM presented the main elements of a study[15] 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) are not taken on the basis of data transferred from the EU.**

70. 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).

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

71. **However, the study at the same time underlines that this is a fast developing area which still has to be closely monitored in the future.**

72. Some private companies (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions[16]. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.

73. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.

74. The FTC publicly announced that they are investigating the Equifax data breach case[17].

75. The FTC also presented the RealPage company case[18], which is offering background screening services by conducting criminal checks and automated decisions making by using weak accuracy verification methods[19]. The FTC asked the company to put in place a better, reasonable procedure to ensure first names' accuracy. This case led to a 3 million dollars fine settlement[20].

76. There was no other significant new developments as regards Automated Decision Making to take note of.

77. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling and 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 request reconsideration on a non-automated basis where an actual need for additional safeguards is identified.**

---

[16] See for example the "Prism Analytics" tool offered by Workday which allows companies to "bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization" (see https://www.workday.com/en-us/applications/prism-analytics.html) and the AI-based predictive marketing tool "Einstein" proposed by Salesforce (see: https://www.salesforce.com/products/einstein/overview/).

[17] See: https://www.ftc.gov/equifax-data-breach (last accessed on 28 November 2018).

[18] See: https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed (last accessed on 28 November 2018).

[19] According to the abovementioned US FTC's press release: *"(...) RealPage compiled screening reports through an automated system that used the applicant's first name, middle name when available, last name, and date of birth when searching for criminal records. Its matching criteria only required an exact match of an applicant's last name along with a non-exact match of a first name, middle name, or date of birth, the FTC alleges. For example, if RealPage searched an applicant named Anthony Jones born on October 15, 1967, it would deem a match if it found a criminal record for Antony Jones 10/15/67, Antonio Jones 10/15/67 and Antoinette Jones 10/15/67."*

[20] See: https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc

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

4.1 Introduction

78. **The EDPB welcomes that the U.S. government has continued to publish a number of important documents**, e.g. decisions by the Foreign Intelligence Surveillance Court[21] (FISA Court), in part by declassification, as well as through the new website set up. These publications and declassifications continue to demonstrate the efforts by the U.S. government and of the U.S. legislator to become more **transparent** about the use of surveillance powers. In addition, these documents help to better understand how the various surveillance programs are operated, including their safeguards. The additional explanations and answers provided during the two Joint Reviews also helped the EDPB to get a clearer understanding of these programs and safeguards and of their concrete impact on the level of data protection in place.

79. Nevertheless, some of the main points of concern that the WP29 expressed in its 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 more detailed analysis.**

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

4.2.1 Collection of data for national security purposes under Section 702

80. In its Schrems judgment[22], the CJEU recalled 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"*[23] 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"*[24].

81. **The previous concerns expressed by the WP29 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. Therefore the EDPB recalls the concerns expressed previously by the WP29 in this respect.

82. The **EDPB also regrets that in the context of the re-authorization of section 702 FISA last year, the US legislator did not take the opportunity to introduce additional safeguards**.

83. The EDPB thus maintains its call for further independent assessment on the necessity and proportionality of the definition of "targets" and of the tasking of selectors under section 702 (including in the context of the UPSTREAM program), as well as the concrete process of application of

[21] U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)
[22] Case C-362/14, 5 October 2015
[23] See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.
[24] See recital 94.

selectors in the context of the UPSTREAM program to clarify whether massive and indiscriminate access to personal data of non-U.S. persons takes place.

84. **The EDPB would welcome if the Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency with a quorum (see infra), should now be in a position to prepare and issue an updated report on Section 702, building on the report issued in 2014.**

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

85. **In the context of the second Joint Review, given the disagreements between the EDPB, on the one hand, and the European Commission and the US authorities on the other, as to the relevance of Executive Order 12333 for the adequacy decision, the application of legislation was not further discussed.**

86. The EDPB recalls 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**. This is why the WP29 analysed the Executive Order 12333 and the Presidential Policy Directive 28 (PPD-28), which is all the more important in this context as it 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. During the Joint Review, the U.S. authorities underlined again 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.

87. The WP29 welcomed the adoption of PPD-28. The current U.S. government confirmed its commitment during the Joint Review to comply with the rules set therein, which the EDPB welcomes. Indeed, the PPD-28 provides limitations to the collection of data, as the signal intelligence activities have to be as "tailored as feasible". The EDPB notes that the recently published report by the PCLOB on PPD-28 confirms that it has been transposed into the internal policies of the relevant authorities. **However, neither the report nor the Second Joint Review provided substantial new information concerning the application of this text,** especially on the interpretation of the six purposes allowing for the use of data foreseen in this text, or on additional elements as to the amount of personal data collected in order to allow for a validation of the commitments and the assurances provided. Here again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB would welcome if the PCLOB finished and issued its awaited report on EO 12333 to provide information on the concrete operation of this Executive order and on its necessity and proportionality.

88. In addition, a more detailed follow-up report on how the PPD-28 applies to the different surveillance programs would be welcome to provide additional elements on these aspects.

4.3 Oversight

89. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, as the CJEU and the ECtHR have also emphasized in many judgments.

90. **Additional presentations were made during the second Joint Review by the different institutions of which the oversight structure consists. Although these elements brought few new elements, they**

confirmed the understanding of the EDPB, of the architecture and functioning of the Inspector General community.

91. Already during the first annual Joint Review, the WP29 was presented with the oversight activities of several entities and considers that a **comprehensive internal oversight structure**, independent from the Intelligence Community, is in place, including the Privacy and Civil Liberty officers, the oversight of the Department of Justice, and Inspector Generals, amongst others.

92. As expressed in the previous opinions of WP29, the EDPB is aware of the complex and multi-layered oversight structure established in the U.S. in order to ensure that personal data is collected and processed in accordance with U.S. law. As underlined in the previous report of the WP29, the EDPB remains of the view that the offices of **the Inspector Generals**, institutions rarely known in most EU Member States, provide valuable checks on the US government's agencies.

93. **The EDPB welcomes the appointment of a new Chair as well as of two new members of the PCLOB. This means that the PCLOB has reached the required quorum for its functioning just before the second Joint Review, although the remaining vacant positions and the requirement for this organ to be bipartisan are yet to be fulfilled.** 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 a particularly helpful source to understand the functioning of the various programs, as an independent body, to be an essential element of the oversight structure.

4.4 Redress for EU individuals

94. In its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal[25]. 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.

95. **As the U.S. government informed during this year's Joint Review that the legal framework remained 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 highest courts in Europe, meaning the CJEU and ECtHR**.

96. As underlined in the previous report of the WP29, 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"**.

97. 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 against 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 provide additional guarantees concerning the effectiveness of judicial redress offered before U.S. courts. However, as was confirmed during the Joint Review, the interpretation of the notion of "standing" in surveillance matters is evolving with cases still pending[26].

[25] See paragraph 95

[26] See in particular cases ACLU v. Clapper, and Wikimedia v. NSA

4.5 Ombudsperson mechanism

98. **The most significant element in the context of the second Joint Review was the nomination of a new acting Ombudsperson, Mrs Manisha Singh, on 28 September 2018.**

99. Since the effective remedy before an independent tribunal is of such importance in the jurisprudence of the European courts, the WP29 welcomed the establishment of an **Ombudsperson** mechanism as a new redress mechanism in its previous opinion. It underlined that this may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. The Ombudsperson mechanism complements the possibilities of redress, or 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. In addition, as the PPD-28 does not create rights, it was confirmed that the individual cannot go to court based on an alleged violation of the PPD-28. Thus, the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument is to ask the Ombudsperson to refer the matter to the competent Inspector General to check the internal policies of these authorities.

100. With Art. 47 of the Charter of Fundamental Rights in mind, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high. Having analysed the jurisprudence of the ECtHR in particular, the WP29 took into account the powers of the Ombudsperson, in particular the powers to access information as well as to remedy non-compliance. When assessing the Ombudsperson mechanism in its opinion and its report of last year, the WP29 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.

101. During the first and the second Joint Review, as well as before the EDPB Plenary in July 2018, the previous and new acting Ombudspersons 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 two acting Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and Mrs Singh also underlined during the second Joint Review that she could escalade the issue should she be unconvinced by the outcome presented to her following the assessment of a request. While the EDPB still has no reason whatsoever to doubt the integrity of the new (acting) Ombudsperson, **it recalls that a permanent Ombudsperson should be appointed as soon as possible as well as its expectation to learn more about the powers that the Ombudsperson has vis-à-vis the Intelligence Community**. This information however 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. The EDPB acknowledges that the acting Ombudsperson explained how a theoretical case would be handled during the Joint Review.

102. Based on the available information, the EDPB still doubts that the powers to remedy non-compliance vis-à-vis the intelligence authorities are sufficient, as the "power" of the Ombudsperson seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the (acting) Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfil their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, it was confirmed during the Joint Review that the decisions of the Ombudsperson cannot be brought to court.

103. The EDPB recalls 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. **As a conclusion, the EDPB is not be in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not 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.**[27]

4.6 Access to data for law enforcement purposes

104. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure seem to imply that data are accessed for a specific purpose and that individuals are notified that their data have been accessed within the framework of criminal proceedings, in the context of which they can have access to judicial redress. However, it recalls its concerns as regards effective remedies available to individuals in cases where the data processed by companies is accessed by law enforcement authorities, as underlined in the previous opinion issued by the WP29[28].

5 CONCLUSION

105. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions,** as well as the efforts made by the U.S Government by publishing a number of important documents **and the appointment of a new Chair as well as of two new members of the PCLOB, meaning that the PCLOB has reached the required quorum for its functioning.**

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

107. **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 processors, as well as the recertification process.** 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.

108. As regards the **collection of data by public authorities**, **the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.

109. **On the Ombudsperson mechanism**, the EDPB is **still awaiting the appointment of a permanent independent Ombudsperson**. Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not 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**.

[27] A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.
[28] WP 238

110. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending** before the Court.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

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

Factual findings of the second 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 3944 organizations, 338 are on the "Inactive" List either because they have withdrawn from the program (38), not recertified or because their certification has lapsed. There was no case where an organization was removed from the List because it persistently failed to comply.
3. GDPR has led to an increase of interest in the Privacy Shield. The DoC has about 1000 more certifications under review.
4. The DoC has increased their staff to 12 persons now that exclusively work on the Privacy Shield.

1 ON COMMERCIAL ASPECTS

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

5. 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
6. DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled.
7. 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 because they consider that the Privacy Shield does not go into this level of detail.
8. 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.
9. The DoC now:
    - 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

10. As the practical experience with the certification process increases the DoC has refined their procedures and now for example have produced more guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links 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.

11. 2 weeks before a certification reaches its next certification due date, the DoC sends the organization a notice to remind them of the need to re-certify if the organization wishes to stay on the "active" List.

12. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date.

13. However, the re-certification process is usually not finished by the due date which leads to organizations being listed as "active" while the due date for re-certification has "expired". A very common reason for this is for example an unpaid fee. The DoC then has to go back to the organization to explain what needs to be done.

14. The DoC emphasized that even if the due date for re-certification on the Privacy Shield list is in the past, there is no gap in the protection because the protection is provided by the public commitments made by the organizations.

15. However they agreed that this situation might be confusing for companies or individuals checking the listing of an organization and seemed to agree that it would at a minimum be helpful if the Privacy Shield website itself would provide an explanation on why an organization is still on the "active" list while the due date for the re-certification has expired.

16. Once the organization has submitted its application for re-certification it is required to complete its certification within 45 days. If it fails to meet this deadline, it is required to remove any references to its participation in the Privacy Shield Program and it might face referral to the FTC.

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

17. On a quarterly basis the DoC identifies organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.

18. 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 to 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.

19. 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.

20. 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 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 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.

21. As an example, the DoC indicated that Facebook and Cambridge Analytica were for instance removed from the list for some processing because they lapsed.

22. In addition, the DoC clarified that concerning the Facebook data breach, the certificate to the Privacy Shield of Facebook does not cover the platform from which the app accessed the data.

23. 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.

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

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

26. **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 Oversight and supervision of compliance with the principles - Activities by the FTC

27. FTC now has 5 commissioners again.

28. The new commission is organizing hearings on Competition and Consumer Protection in the 21st Century which will also cover the existing and possible extension of the FTC´s enforcement powers (https://www.ftc.gov/policy/advocacy/public-comment-topics-process#5).

29. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers working only on privacy (a few also work on FOIA) and there are more people from other fields (e.g. tech) that support their work.

30. This year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification, 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.

31. The FTC has started to send out CIDs (Civil Investigation Demands) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the

FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.

32. The FTC still practices the already established procedure to check the cases it investigates for other reasons if the organization is also certified under the Privacy Shield.

33. With regards to the ongoing investigation concerning Facebook and Cambridge Analytica, the FTC was not in a position to share any detail. However, the Chief Council of the DoC shared verbally the content of an early response letter from Facebook in which the company basically presented different points of its line of defence.

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

34. Currently there is no airline participating in the Privacy Shield and only very few ticket agents.

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

1.5 Guidance for the companies adhering to the Privacy Shield

36. The DoC has (following informal consultation of members of the ITS at working level) produced guidance on the Accountability for Onward Transfer Principle and the notion of Processor and published it on its website

1.6 IRM

37. The DoC has issued guidance to the IRM in order to have comparable annual reports.

38. The DoC plans to issue guidance on possible conflicts of interest for the next year.

39. Most complaints to the IRM VeraSafe were found ineligible because the complainant was an U.S. resident and the company concerned was also situated in the U.S.

40. As contractually agreed, if there was a breach in the Privacy policy (meaning if the company did not respect its privacy policy, not that the policy itself is in breach of the Privacy Shield), the VeraSafe clients (organizations that certified under the privacy shield) committed to accept VeraSafe's decision to impose a "fine" on them. The "fine" would be paid to the individual that successfully claimed a breach.

1.7 Arbitral Panel

41. The fee, that according to the Privacy Shield text is collected from the certified organizations annually is actually only collected once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to 4.5 million $.

42. Arbitral panel procedure has never been triggered so far. The question is if the fee should still be collected. Recommendation of the Arbitral Administrator Association (that manages the fund) is to not change anything for now since there is no figure on how much the handling of an average case would cost.

1.8 Automated Decision Making

43. The COM presented the main elements of a study commissioned to an independent contractor.

44. The study came to the conclusion that automated decisions making (in the narrow GDPR definition of decisions having legal effects on individuals), these decisions are not taken on the basis of data transferred from the EU. Such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

45. However, the study at the same time underlines that this is a fast developing area which has to be closely monitored in the future.

46. In the rare situation where ADM are made (for example in the context of credit lending, housing, employment), cases where personal data transferred from the EU are used is quite limited.

47. Some private companies who participated in the joint review exercise (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions[29]. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.

48. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.

49. FTC publicly announced that they are investigating Equifax.

50. The US FTC presented the case about "Realpage", a background screening company doing criminal checks which was conducting automated decisions making by using weak accuracy verification methods (if the last name and the first three letters of the firstname of an individual matched a criminal record, Realpage would consider this enough to identify the individual as criminal). The FTC asked the company to put in place a better, reasonable procedure to ensure firstnames' accuracy. The case led to a 3 million dollars fine settlement[30].

51. There was no other significant new developments as regards Automated Decision Making to take note of.

1.9 HR Data

52. Since the work on guidance regarding the processing of employment data within the last year was not successful this year's review focused less on the definition of HR data but rather on the consequences the different definitions lead to: The worry on the EU side being, that additional protections granted by the Privacy Shield for employment data (Opt In in marketing purposes rather than opt out) would

[29] See for example the "Prism Analytics" tool offered by Workday which allows companies to "bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization" (see https://www.workday.com/en-us/applications/prism-analytics.html) and the AI-based predictive marketing tool "Einstein" proposed by Salesforce (see: https://www.salesforce.com/products/einstein/overview/).
[30] See: https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc

not fall under anyone's jurisdiction. Given the wording of the Privacy Shield, the discussions on different possible readings of this need to continue.

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

53. Legal framework has not changed substantially.

2.1 Reauthorisation of 702 FISA

54. The U.S. government reported about the amendments authorized by the FISA Amendments Reauthorization Act of 2017.

55. In particular, further explanation was provided about the possibility to reintroduce "about collection". It was stressed that, if the governments were to re-introduce "about collection" under the UPSTREAM programme, it would be required to take particularly demanding procedural steps (implying authorizations by the Court and the Congress), and where the FISA Court would be expected to appoint an amicus curiae when such an application is made.

56. The U.S. government also reported about the several transparency requirements, including semi-annual reports, which – together with additional material – is made available on a new website: https://www.intel.gov/intel-vault.

2.2 PPD-28

57. The U.S. government published a response to the recently published (in redacted form) report by the PCLOB. It disagrees with the PCLOB on the question of whether the scope of application of PPD28 is sufficiently clear for the agencies to apply it (PCLOB expressing doubts in the said report).

58. The U.S. government confirmed that the safeguards of PPD-28 also apply for personal data collected under 702 FISA. This would include safeguards related to the retention of data, their dissemination, and specifications on the targeting with regard to the purpose of collecting foreign intelligence.

2.3 The Ombudsperson mechanism and the EU individual complaint handling body

59. Acting Under Secretary of State for Economic Growth, Energy, and the Environment and Acting Privacy Shield Ombudsperson, Manisha Singh, explained the procedures set up to make the Ombudsperson mechanism under the Privacy Shield work, including how a case would be handled in theory. No further declassified information was shared as to the rules of procedure of how she cooperates with the intelligence community. She assured she would not sign a response letter to the requestor if she were not convinced of the findings presented to her. It was confirmed during the discussion that, in response to an Ombudsperson request, she would be provided with a report from the Intelligence Community (IC) in order to provide oversight and to take actions (without being able to directly access information or directly remedy non-compliance). She also stressed that she would have the ability to escalate the matter to the Secretary of State in order to assure that her demands are met.

60. The European Centralised Body (EUCB) presented its rules of procedure, explaining how a request would be handled before submitted to the Ombudsperson.

61. A representative of the Intelligence Community (IC) confirmed that the Inspector General of the ODNI would always be informed when a request would be forwarded to the ODNI by the Ombudsperson.

62. As the remedying of a possible violation, the U.S. government clarified that any violation of FISA would also have to be reported to the FISA court.

2.4 PCLOB

63. Shortly before the second annual review, the Senate confirmed three members of the PCLOB. As President Trump appointed those candidates on 16 October 2018, the PCLOB has reached quorum again. Two additional candidates have been nominated and are awaiting their confirmation by the U.S. Senate.

64. In addition, also shortly before the joint review, the PCLOB published a redacted version of its report on PPD-28. The government also published a response to that report.

65. The new PCLOB will have to decide about the declassification of report on Executive Order 12333 finalized under the previous PCLOB Chair.

66. As regards other reports to be done, and possible reviews of previous report, such as on section 702, the new PCLOB would have to determine in the coming times its work plan and schedule.

2.5 Inspector General (IG) of the ODNI

67. The new IG was sworn in on 17 May 2018. He stressed his independence and the fact that he has full access to (classified) documents in the IC community, which would as a matter of fact never be restrained.

68. He clarified that usually indirect access to information would be sought through reports from the IC community, but that the IG has direct access as well, if needed.

69. He also confirmed that IG, in principle, has discretion whether to act and would follow set priorities, but that requests by the Ombudsperson would in the current setting always be considered as of particular importance.

2.6 Redress

70. The U.S. government presented recent case law of the FISA court and referred to the website of the FISA court, where redacted decisions are published.

71. Related to the procedural requirement of “standing”, the U.S. government reported about the ACLU case, decided by different FISA “chambers” and finally on the appellate level. It deals with an unusual case, where ACLU was seeking the publication of FISA court decisions, based on a right of public access to documents. The court had denied in the first instance that ACLU would have standing. Finally, the FISA Court of Review court said it would.

72. No further developments could be presented on the requirement of standing in other relevant cases, as the Wikimedia case is still pending. With regard to legal claims relying on a violation of FISA, the U.S. Government referred to the possibility of making a Freedom of Information (FOIA) request first.

73. The U.S. confirmed that PPD-28 does not create rights enforceable before a court. Consequently, cases would have to be brought to the attention of the IG or the Ombudsperson.

2.7 Additional information on access to data by law enforcement authorities

74. The U.S. government reported about a Department of Justice memo on the Stored Communications Act[31]. The purpose of the memo would be to further harmonize the use of such applications to the court which prohibit providers to disclose the order. According to the new memo, such applications have to be further justified by the prosecutors seeking such order, and a general limit of 1 year for such orders is foreseen, with exceptions that need to be justified again.

75. The U.S. government also reported about the Supreme Court ruling in the Carpenter case, in which a suspect was prosecuted on the basis cellphone location records, without a search warrant. The Supreme Court ruled that the evidence was illegally acquired and not receivable in court, since the suspect had a reasonable expectation of privacy for these data so that the government had violated the Fourth Amendment to the United States Constitution by accessing the cellphone location records without a search warrant. [32]

[31] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).
[32] Carpenter v. United States, 138 S. Ct. 2206