EUROPEAN
COMMISSION

Brussels, 23.10.2019
COM(2019) 495 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the third annual review of the functioning of the EU-U.S. Privacy Shield

{SWD(2019) 390 final}

1. THE THIRD ANNUAL REVIEW – BACKGROUND, PREPARATION AND PROCESS

On 12 July 2016, the Commission adopted a Decision (the "adequacy decision") in which it found that the EU-U.S. Privacy Shield ensures an adequate level of protection for personal data that has been transferred from the EU to organisations established in the U.S..[1] The adequacy decision notably requires the Commission to carry out an annual review to evaluate all aspects of the functioning of the framework, and, on that basis to prepare a public report to be submitted to the European Parliament and the Council.

The first annual review took place in September 2017 in Washington, D.C., and in October 2017 the Commission adopted its report to the European Parliament and the Council,[2] accompanied by a Commission Staff Working Document (SWD(2017)344 final).[3] The Commission concluded that the United States continued to provide an adequate level of protection for data transferred from the EU to the U.S. under the Privacy Shield, but made ten recommendations to improve the practical functioning of the framework.

The second annual review was carried out in October 2018 in Brussels, and the Commission adopted its report to the European Parliament and the Council in December 2018,[4] again accompanied by a Commission Staff Working Document (SWD(2018) 487 final).[5] The information gathered in the context of the second annual review confirmed the Commission's findings in the adequacy decision, both with regard to the "commercial aspects" of the framework (i.e. aspects relating to certified companies' compliance with the Privacy Shield requirements as well as to the administration, oversight and enforcement of such requirements by the competent U.S. authorities) and with regard to aspects concerning public authority access to personal data transferred under the Privacy Shield.

In particular, the steps taken to implement the Commission's recommendations following the first annual review had improved several aspects of the functioning of the framework in practice. For instance, the Department of Commerce had introduced new mechanisms to detect potential compliance issues, the Federal Trade Commission had adopted a more proactive approach to compliance monitoring and enforcement, and the report of the Privacy

[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] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield (COM(2017)611 final), see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[3] Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2017)344 final), see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[4] Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield (COM (2018) 860 final), see https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

[5] Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2018)497 final), see https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf.

and Civil Liberties and Oversight Board on the implementation of Presidential Policy Directive 28[6] had been publicly released. However, as some of these steps had been taken just before the second annual review and certain processes were still ongoing, the Commission concluded that further developments concerning these processes and mechanisms required close monitoring.

Moreover, while the function of the Ombudsperson under the Privacy Shield was carried out by the Acting Under Secretary of State and the Ombudsperson mechanism was thus fully functioning, the Commission stressed the importance of filling the position of Privacy Shield Ombudsperson on a permanent basis and, in particular, called on the U.S. government to identify a nominee for this position before 28 February 2019.

The third annual review meeting took place in Washington, DC on 12 and 13 September 2019. It was opened by Director-General for Justice and Consumers Tiina Astola, U.S. Secretary of Commerce Wilbur Ross, Chairman of the Federal Trade Commission Joseph Simons and Vice Chair of the European Data Protection Board Ventsislav Karadjov. For the EU, the meeting was conducted by representatives of the European Commission's Directorate General for Justice and Consumers. Eight representatives designated by the European Data Protection Board[7] also participated in this meeting.

On the U.S. side, representatives from the Department of Commerce, the Department of State, the Federal Trade Commission, the Department of Transportation, the Office of the Director of National Intelligence, the Department of Justice and members of the Privacy and Civil Liberties Oversight Board participated in the review, as well as the newly appointed Ombudsperson (on a permanent basis, see below) and the Inspector General for the Intelligence Community. In addition, representatives from two organisations that offer independent dispute resolution services under the Privacy Shield and the American Arbitration Association, which administers the Privacy Shield arbitration panel, provided information during the relevant review sessions. Finally, presentations by Privacy Shield-certified organisations on the steps that companies take to comply with the requirements of the framework also informed the annual review.

In preparation for the third annual review, the Commission had gathered information from relevant stakeholders (in particular Privacy Shield-certified companies through their respective trade associations and non-governmental organisations active in the field of fundamental rights, in particular digital rights and privacy). In addition to the collection of written input, the Commission had meetings with industry and business associations on 9 September 2019 and with non-governmental organisations on 11 September 2019.

The Commission's findings have been further informed by publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from non-governmental organisations, transparency reports issued by Privacy Shield-

[6] Presidential Policy Directive 28: Signals Intelligence Activities, 17 January 2014, which provides important limitations and safeguards for non-U.S. persons in the area of signals intelligence collection.

[7] The independent body bringing together representatives of the national data protection authorities of the EU Member States and the European Data Protection Supervisor.

certified companies, annual reports from independent recourse mechanisms, as well as media reports.

The present report concludes the third annual review of the functioning of the Privacy Shield. The report, as well as the accompanying Staff Working Document (SWD(2019)390 final), follow the same structure as the documents on the two previous reviews. It covers all aspects of the functioning of the Privacy Shield, with a particular focus on those elements that the Commission had identified during the second annual review as requiring close monitoring.

In conducting its assessment, the Commission also took into account further developments that occurred over the last year, including the pending litigation relating to the Privacy Shield before the Court of Justice of the European Union.[8] In this respect, the review provided an opportunity for the Commission to obtain clarifications from the U.S. authorities on certain specific aspects of the U.S. legal framework governing the collection of foreign intelligence information, that were raised in the context of the so-called *Schrems II* case. Nevertheless, once the Court rules on the pending cases, the Commission may have to reassess the situation.

2. FINDINGS

In its third year of operation, the Privacy Shield, which at the time of the annual review meeting had more than 5,000 participating companies, has moved from the inception phase to a more operational phase. Covering both commercial aspects and issues relating to government access to personal data, the third annual review focused on the experience and lessons learnt from the practical application of the framework.

The detailed findings concerning the functioning of the Privacy Shield framework after its third year of operation are presented in the Commission Staff Working Document on the third annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2019)390 final) which accompanies this report.

2.1. Commercial aspects

In light of the findings of last year's annual review, the Commission's assessment of the commercial aspects focused notably on the progress made by the Department of Commerce on (i) the re-certification process, (ii) the effectiveness of the mechanisms introduced by the Department of Commerce to proactively monitor compliance by the certified companies (the so-called "spot-checks"), (iii) the tools introduced to detect false claims, (iv) the progress and outcome of Federal Trade Commission enforcement actions regarding violations of the Privacy Shield, and (v) the developments concerning the guidance on human resources data.

With respect to the *re-certification process*, it emerged at the third annual review that as a regular practice, at the expiration of the (re)certification period, if a company has not yet completed the re-certification process, the Department of Commerce, following an internal

[8] See case T-738/16 La Quadrature du Net v. Commission. Questions on the Privacy Shield have also been raised in the context of case C-311/18 Data Protection Commissioner and Facebook Ireland, Maximilian Schrems ("*Schrems II*"), in which a hearing took place before the Grand Chamber of the Court of Justice on 9 July 2019.

procedure, grants to the company a "grace period" of a significant length. During this period (for approximately 3.5 months, or, in some instances and depending on when the Department of Commerce detects that the re-certification process was not completed, even a longer period of time), the company remains on the Privacy Shield "active" list. For as long as a company is listed as participating in the Privacy Shield, the obligations under the framework remain binding and fully enforceable. However such a long period in which a company's re-certification due date has lapsed while the company continues to be listed as active Privacy Shield participant reduces the transparency and readability of the Privacy Shield list for both businesses and individuals in the EU. It also does not incentivise participating companies to rigorously comply with the annual re-certification requirement.

With respect to *proactive checks of companies'* compliance with the Privacy Shield requirements, the Department of Commerce introduced in April 2019 a system in which it checks 30 companies each month. The Commission welcomes that the Department of Commerce is carrying out proactive compliance spot-checks on a regular basis and in a systematic manner, which is very important for improving the overall compliance with the framework and for detecting cases that require enforcement action by the Federal Trade Commission. However, it notes that these spot-checks tend to be limited to formal requirements such as the lack of response from designated points of contact or the inaccessibility of a company's privacy policy online. While these are certainly relevant aspects of compliance with the Privacy Shield's requirements, such checks should also cover substantive obligations, for example, compliance with the Accountability for Onward Transfers Principle making full use of the instruments the Department of Commerce can rely on under the framework. The requirements for onward transfers have been significantly strengthened in the Privacy Shield, as a lack of safeguards in such situations would undermine the protections guaranteed by the framework. Whereas the spot-checks should continue to be done regularly and in a systematic manner, compliance with these more substantive requirements is also crucial for the continuity of the Privacy Shield and should be subject to strict monitoring and enforcement by the U.S. authorities.

With respect to the Department of Commerce's *search for false claims* of participation in the Privacy Shield, the Commission noted that the Department of Commerce had continued to conduct searches on a quarterly basis, which has led to the detection of a significant number of cases of false claims, which in some instances were also referred to the Federal Trade Commission. However, these searches have so far only been aimed at companies that had in some way already been certified or applied for certification under the Privacy Shield (but, for example, were not re-certified). It is important that they also target companies that have never applied for certification under the Privacy Shield. From all kinds of false claims, the false claims from companies that never applied for certification are potentially the most harmful. This is true from the point of view of individuals' privacy, as companies that have never applied for certification have not implemented any of the protections guaranteed by the Privacy Shield in their business practices. It is also true from a business' perspective, since the level playing field between companies is weakened if organisations, which are not complying with the requirements of the framework, can claim the benefits of certification.

The Commission positively noted that an increasing number of EU data subjects are making use of their rights under the Privacy Shield and that the relevant redress mechanisms function well. The number of complaints submitted to independent recourse mechanisms increased and were resolved to the satisfaction of the EU individuals concerned. Moreover, requests from EU individuals were appropriately handled by participating companies.

As regards *enforcement*, the Commission noted that since last year, the Federal Trade Commission concluded seven enforcement actions related to Privacy Shield violations, including as a result of the announced *ex officio* sweeps. All seven cases concerned false claims of participation in the framework. Two of these cases were also about the violation of more substantive requirements of the Privacy Shield, such as the failure to verify through a self-assessment or by means of an outside compliance review that the assertions the company makes about its Privacy Shield practices are true and that those practices have been implemented. The Commission welcomes the enforcement action taken by the Federal Trade Commission in the third year of operation of the Privacy Shield. At the same time, in light of the agency's announcement of last year and the assurances provided in the course of the second annual review, the Commission would have expected a more vigorous approach regarding enforcement action on substantive violations of the Privacy Shield Principles.

In that respect, the Commission took note of the explanation given at the third annual review that a number of ongoing investigations are taking more time, as the Federal Trade Commission is looking at the full range of possible violations. However, the information provided by the Federal Trade Commission was too limited to appropriately evaluate progress in enforcement. While such information may be restricted for legitimate confidentiality considerations, it does not appear justifiable that the Federal Trade Commission cannot share, even in an aggregate and anonymous form, more elements on the *ex officio* sweeps that are being carried out. This approach is not in line with the spirit of cooperation among authorities on which the Privacy Shield is based, and the Federal Trade Commission should find ways to share meaningful information on its enforcement activity, with the Commission and n with the EU Data Protection Authorities that are co-responsible for the enforcement of the framework.

The issue of how *human resources data* is handled under the Privacy Shield was again discussed during the review. As confirmed by stakeholders, the development of joint guidance between the Department of Commerce, Federal Trade Commission and the EU Data Protection Authorities would be of real added value. In this respect, the Commission notes that contacts have recently taken place and have led to some progress in the understanding of the issues, but without having resulted in any concrete outcome yet.

2.2. Access and use of personal data by U.S. public authorities

Regarding aspects relating to access and use of personal data by U.S. public authorities, the third annual review was, first of all, aimed at confirming that all the limitations and safeguards that the adequacy decision relies on remain in place. In addition, the third annual review provided an opportunity to look at new developments and to further clarify certain aspects of the legal framework, as well as the different oversight mechanisms and the

possibilities for redress, in particular with respect to the handling and resolution of complaints by the Ombudsperson.

While there were no new legal developments concerning the *collection of foreign intelligence information* pursuant to Section 702 of the Foreign Intelligence Surveillance Act, the Commission welcomed the clarifications received by the U.S. authorities on the way in which the collection of intelligence information is targeted under the intelligence programmes carried out pursuant to Section 702 of the Foreign Intelligence Surveillance Act (i.e. Prism and Upstream). These clarifications confirmed the Commission's findings in the adequacy decision that the collection of foreign intelligence information under Section 702 of the Foreign Intelligence Surveillance Act is always targeted through the use of selectors, and that the choice of selectors is governed by law, subject to independent judicial and legislative oversight.

The Commission also noted that some of the authorities for obtaining foreign intelligence information under Section 501 of the Foreign Intelligence Surveillance Act, as modified by the USA FREEDOM Act of 2015, are scheduled to expire on 15 December 2019. Since the collection under Section 501 of the Foreign Intelligence Surveillance Act is relevant in the context of the Privacy Shield and has therefore been assessed in the Commission adequacy decision, it is important that in case of reauthorization, the existing limitations and safeguards, such as the prohibition of bulk collection, remain in place.

With respect to *Presidential Policy Directive 28*, the U.S. authorities explicitly confirmed that it remains in full force and effect and has not been subject to any amendments. There have also been no modifications to the procedures implementing Presidential Policy Directive 28 within the different agencies of the Intelligence Community. Moreover, the Commission took note of the explanations provided by the U.S. authorities, clarifying that the provisions on bulk collection in Presidential Policy Directive 28, including those on temporary acquisition, do not apply to the collection of foreign intelligence information within the U.S. (for example, to the collection of information from a certified company processing data transferred from the EU under the Privacy Shield), such as collection carried out under Section 702 of the Foreign Intelligence Surveillance Act under the Prism or the Upstream program, as this collection is always targeted.

As regards the *Privacy and Civil Liberties Oversight Board*, an important oversight body in the area of government surveillance, the Commission welcomed that with the recent confirmations of two additional Board members by the U.S. Senate, the Privacy and Civil Liberties Oversight Board for the first time since 2016 has a full slate of five members. The Commission also noted that the Board's staff has doubled since the last annual review, and that it has adopted an ambitious work programme consisting of ten ongoing oversight projects, some of which are of particular relevance for the Commission's periodic review of the Privacy Shield.

With respect to the Privacy Shield *Ombudsperson mechanism*, the U.S. President announced on 18 January 2019 the nomination of Keith Krach as the Under Secretary of State who also

serves as the Ombudsperson. On 20 June 2019, Mr Krach was confirmed by the Senate. The Commission welcomes the appointment of Mr Krach as Privacy Shield Ombudsperson, which ensures that the position is filled on a permanent basis.

As regards the first complaint to the Ombudsperson mechanism that had been submitted via the Croatian Data Protection Authority just before the last annual review, this complaint was eventually found inadmissible, as it related to facts that were completed before the Privacy Shield decision was adopted. Nevertheless, the complaint offered an opportunity to test the functioning of the relevant procedures in practice. Both the European Data Protection Board representatives to the annual review and the Ombudsperson confirmed that all relevant steps of the procedure had been triggered and completed in a satisfactory manner. The Commission welcomes the successful processing of this first request as an important indication that the Ombudsperson mechanism can properly perform its functions.

The U.S. authorities also provided further explanations on how the Ombudsperson would work with other independent oversight bodies and how it would remedy violations. They notably confirmed that the independent Inspector General of the Intelligence Community would be systematically informed of any complaint submitted to the Ombudsperson, and would carry out his own assessment. In addition, they explained that if a complaint before the Ombudsperson would reveal a violation of the targeting procedures under section 702 of the Foreign Intelligence Surveillance Act such a violation would be reported to the Foreign Intelligence Surveillance Court, which would carry out an independent review and, if necessary, order the relevant intelligence agency to take remedial action. This remedy may range from individual to structural measures, e.g. from the deletion of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training of staff.

Finally, it was confirmed that, if a violation of U.S. law (including a violation of Executive Orders, Presidential Policies and agency rules and procedures, such as e.g. the targeting and minimisation procedures approved by the Foreign Intelligence Surveillance Court) would be identified in the course of the review of a complaint to the Ombudsperson, the unlawfully collected data would be purged from all government databases and any reference to that data would be removed from intelligence reports. An individual in the EU would thus be able to obtain the deletion of his or her personal data if it was unlawfully collected and processed by the U.S. Intelligence Community.

The Commission welcomes these additional explanations, which demonstrate how cooperation between the different independent oversight bodies strengthens the efficiency of the Ombudsperson mechanism. It was also important to clarify that by using the Ombudsperson mechanism, individuals in the EU can in fact exercise their right to deletion, which is a fundamental element of the right to the protection of personal data.

3. CONCLUSION

The information gathered in the context of the third annual review confirms the Commission's findings in the adequacy decision, both with regard to the commercial aspects of the framework and with regard to aspects relating to access to personal data transferred under the

Privacy Shield by public authorities. In this respect, the Commission noted a number of improvements in the functioning of the framework as well as appointments to key oversight bodies.

However, in light of some issues that emerged from the day-to-day experience or became more relevant in the context of the practical implementation of the framework, the Commission concludes that a number of concrete steps need to be taken to better ensure the effective functioning of the Privacy Shield in practice:

1. The Department of Commerce should shorten the different time periods that are granted to companies for completing the re-certification process. A period of maximum 30 days in total would seem reasonable to allow companies sufficient time for re-certification, including for rectifying any issue identified in the re-certification process, while at the same time ensuring the effectiveness of this process. If at the end of this period the re-certification is not completed, the Department of Commerce should send out the warning letter without further delay.

2. In the context of its spot-check procedure, the Department of Commerce should assess companies' compliance with the Accountability for Onward Transfers Principle, including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer.

3. As a matter of priority, the Department of Commerce should develop tools for detecting false claims of participation in the Privacy Shield from companies that have never applied for certification, and use these tools in a regular and systematic manner.

4. The Federal Trade Commission should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission, as well as with EU Data Protection Authorities that also have enforcement responsibilities under the Privacy Shield.

5. The EU Data Protection Authorities, the Department of Commerce and the Federal Trade Commission should develop common guidance on the definition and treatment of human resources data in the coming months.

The Commission will continue to closely monitor further developments concerning specific elements of the Privacy Shield framework, notably (i) the functioning of the Ombudsperson mechanism, in particular in case of a new complaint; (ii) the outcome of the ongoing oversight projects that have been initiated by the Privacy and Civil Liberties Oversight Board and that are particularly relevant for the Privacy Shield (for example on the querying of data obtained under Section 702 of the Foreign Intelligence Surveillance Act by the Federal Bureau of Investigation, the implementation of the Board's recommendations on Presidential Policy Directive 28, etc.); (iii) the reauthorisation of Section 501 of the Foreign Intelligence

Surveillance Act, in particular that the existing safeguards remain in place; and (iv) the evolving U.S. case law on judicial redress in the area of government surveillance, in particular with respect to the issue of standing before the courts.

Finally, the Commission will continue to follow closely the ongoing debate about federal privacy legislation in the U.S. A comprehensive approach to privacy and data protection would increase the convergence between the EU and the U.S. systems and this would strengthen the foundations on which the Privacy Shield framework has been developed.