EUROPEAN
COMMISSION

Brussels, 18.10.2017
COM(2017) 611 final

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}

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

1. THE FIRST ANNUAL REVIEW – PURPOSE, PREPARATION AND PROCESS

In its Decision of 12 July 2016[1] ("the adequacy decision"), the Commission found that the EU-U.S. Privacy Shield ("Privacy Shield") ensures an adequate level of protection for personal data that has been transferred from the European Union to organisations in the U.S.

The Privacy Shield reflects the principles and requirements laid down by the European Court of Justice in its decision in the *Schrems* case[2], which invalidated the previous Safe Harbour framework. It provides for a number of novel elements, compared to Safe Harbour, which enhance the protection of personal data when it is transferred to the United States. This includes stricter obligations on Privacy Shield-certified companies, for example regarding limitations on how long a company may retain personal data (so-called "data retention" principle) or the conditions under which data can be shared with third parties outside the framework (so-called "accountability for onward transfers" principle). It also provides for more regular and rigorous monitoring by the Department of Commerce (DoC) and significantly strengthens the possibilities for EU individuals to obtain redress. In addition, the Privacy Shield builds on specific written representations and assurances made by the U.S. government that access by public authorities to personal data transferred under the Privacy Shield for national security, law enforcement and other public interest purposes is subject to clear limitations and safeguards. To this end, it also creates an entirely new redress mechanism, the Ombudsperson.

The Commission committed to evaluate its adequacy finding on an annual basis, and, to this end, conducts an annual review of the functioning of the Privacy Shield. The first annual review of the functioning of the Privacy Shield is concluded with the present report. The review covered all aspects of the Privacy Shield, *i.e*. the implementation, administration, supervision and enforcement of the Privacy Shield framework by the competent U.S. authorities and bodies as well as questions relating to the access by U.S. public authorities to personal data transferred under the Privacy Shield for public interest purposes, in particular national security. It also included a dialogue on the specific topic of automated decision-making and an assessment of developments in the U.S. legal system over the past year which could have an impact on the functioning of 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.

[2] Judgment of the Court of Justice of the European Union of 6 October 2015, Case C-362/14, *Maximilian Schrems v Data Protection Commissioner* ("*Schrems*").

The Privacy Shield framework has been operational since 1 August 2016. Taking into account that this has been the first year of its operation, the Commission's annual review has focused on verifying that all the mechanisms and procedures provided for in the framework – many of which were newly created – have been fully implemented and are functioning in the way that is foreseen in the adequacy decision. Moreover, the Commission has put particular emphasis on checking whether and how the various U.S. authorities involved in the implementation of the framework have lived up to their representations and commitments, both as regards the administration and supervision of the commercial aspects of the Privacy Shield, and with respect to government access to personal data. The change of the U.S. administration in January 2017 made this particularly relevant.

In preparation of the annual review, the Commission gathered information and feedback on the implementation and functioning of the Privacy Shield framework from relevant stakeholders, more specifically from Privacy Shield-certified companies through their respective trade associations, and from non-governmental organisations (NGOs) active in the field of fundamental rights and in particular digital rights and privacy. It also sought and obtained written information from the U.S. authorities involved in the implementation of the framework, including relevant documents and material.

The first Annual Joint Review took place on 18 and 19 September 2017 in Washington, DC. It was opened by Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, and U.S. Secretary of Commerce Wilbur Ross. The annual review was conducted for the EU by representatives of the European Commission's Directorate General for Justice and Consumers. The EU delegation also included eight representatives designated by the Article 29 Working Party, the advisory body bringing together the national data protection authorities of the Member States (DPAs) as well as the European Data Protection Supervisor.

On the U.S. side, representatives of the DoC, the Federal Trade Commission (FTC), the Department of Transportation, the Department of State, the Office of the Director of National Intelligence and the Department of Justice participated in the review, as well as the acting Ombudsperson, a Member of the Privacy and Civil Liberties Oversight Board (PCLOB) and the Office of the Inspector General of the Intelligence Community. Moreover, representatives of organisations that offer independent dispute resolution under the Privacy Shield, the American Arbitration Association as administrator of the Privacy Shield Arbitration Panel and some Privacy Shield-certified companies provided input during the annual review.

The annual review has further been informed by publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from NGOs, transparency reports issued by Privacy Shield-certified companies, press articles and other media reports.

2. FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

The annual review has demonstrated that the U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. The certification process has been handled in an overall satisfactory manner and more than 2400 companies have been certified so far. The U.S. authorities have put in place the complaint-handling and enforcement mechanisms and procedures to safeguard individual rights. This includes also the new additional redress avenues for EU individuals such as the arbitration panel and the Ombudsperson mechanism. Regarding the latter, an Acting Ombudsperson was designated following the change of Administration in January 2017, whereas the nomination of a permanent Ombudsperson is pending. Cooperation with European data protection authorities has been stepped up. As regards access to personal data by public authorities for national security purposes, relevant safeguards on the U.S. side remain in place, notably those based on Presidential Policy Directive 28 issued in 2014 which sets out limitations and safeguards on use by national security authorities of personal data, regardless of nationality of the individual. In this context, it should also be noted that section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) is set to expire on 31 December 2017 and that reform proposals are under discussion in the U.S. Congress.

The detailed factual findings concerning the functioning of all aspects of the Privacy Shield framework after its first year of operation are presented in the Commission Staff Working Document on the annual review of the functioning of the EU–U.S. Privacy Shield (SWD(2017) 344 final) which accompanies the present report.

On the basis of these findings, the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States.

At the same time, the Commission considers that the practical implementation of the Privacy Shield framework can be further improved in order to ensure that the guarantees and safeguards provided therein continue to function as intended.

To this end, the Commission makes the following recommendations:

2.1. Companies should not be able to publicly refer to their Privacy Shield certification before the certification is finalised by the DoC

During the annual review it became apparent that companies which have applied for certification under the Privacy Shield, but whose certification has not yet been finalised by the DoC, can already publicly refer to their Privacy Shield certification. Consequently, there may be a discrepancy between information that is publicly available, and the DoC's Privacy Shield list, which does not include a company before the certification is finalised. Such type of discrepancy creates uncertainty for EU individuals and companies in the EU that want to transfer data to the U.S., increases the risk of false claims of participation and undermines the credibility of the whole framework

Therefore, the Commission recommends that companies should not be allowed to make public representations about their Privacy Shield certification before the DoC has finalised the certification and included the company on the Privacy Shield list. The information provided by the DoC to companies on the certification process, including on the Privacy Shield website, should be amended to clarify that companies cannot publicly refer to their adherence to the framework before being included on the Privacy Shield list.

2.2. Proactive and regular search for false claims by the DoC

The Commission recommends that the DoC conducts, proactively and on a regular basis, searches for false claims of participation in the Privacy Shield, not only in the context of the certification process, *i.e.* with respect to companies that have initiated but not completed the certification and nevertheless already claim participation in the framework, but also more generally with respect to companies that have never applied for certification but make representations suggesting to the public that they comply with the framework's requirements. To this end, the DoC should take additional measures, including internet searches. As learned from the experience of the Privacy Shield's predecessor, the Safe Harbour program, misleading practices are not uncommon and can weaken the credibility and solidity of the system as a whole.

2.3. Ongoing monitoring of compliance with the Privacy Shield Principles by the DoC

The Commission recommends that the DoC conducts compliance checks on a regular basis. Compliance checks could for example take the form of compliance review questionnaires sent to a representative sample of certified companies on a specific "thematic" issue (e.g. onward transfers, data retention), or the DoC could systematically request to be provided with the annual compliance reports (which can be either a self-assessment or on outside compliance review) of certified companies seeking to be re-certified. The DoC could then make use of the annual compliance reports in order to identify possible compliance issues that may warrant further follow-up action before a company can be re-certified, or more systemic deficiencies in the functioning of the framework that need to be addressed.

2.4. Strengthening of awareness raising

The Commission encourages both the DoC and the DPAs to continue and further strengthen the awareness-raising efforts that they have already undertaken in the past year.

In order to ensure more effective protections for EU individuals, the DPAs, in cooperation with the Commission, could strengthen their efforts to inform EU individuals about how to exercise their rights under the Privacy Shield, notably on how to lodge complaints.

2.5. Improve cooperation between enforcers

The Commission recommends that the DoC and the DPAs should cooperate, if appropriate also with the FTC, to develop guidance on the interpretation of certain concepts in the Privacy Shield that need further clarification. This would be in the interest of improved cooperation between the authorities that implement and enforce the framework on both sides of the

Atlantic, of the development of convergence in the interpretation of the Privacy Shield's rules and of greater legal certainty for businesses.

The principle of accountability for onward transfers and the definition of human resources data have emerged from the first annual review as examples of concepts that could benefit from additional clarification.

2.6. Study on automated decision-making

In order to draw more precise conclusions on the question of automated decision-making, including in view of the next annual review, the Commission will commission a study to collect factual evidence and further assess the relevance of automated decision-making for transfers carried out on the basis of the Privacy Shield

2.7. Enshrine the protections of PPD-28 in the Foreign Intelligence Surveillance Act

The upcoming debate on the re-authorisation of Section 702 of the Foreign Intelligence Surveillance Act (FISA) provides the U.S. Administration and Congress with a unique opportunity for strengthening the privacy protections contained in FISA. In this context, the Commission hopes that the Congress will consider favourably enshrining the protections offered by Presidential Policy Directive (PPD)-28 with respect to non-US persons in FISA, with a view to ensuring the stability and continuity of these protections. Any further reforms, both in terms of substantive limitations and in terms of procedural safeguards, should be implemented in the spirit of PPD-28 and thus provide protection irrespective of nationality or country of residence.

2.8. Swift appointment of the Privacy Shield Ombudsperson

The Commission calls on the U.S. administration to confirm its political commitment to the Ombudsperson mechanism, as an important element of the Privacy Shield framework as a whole, by filling the position of the Ombudsperson with a permanent appointee as soon as possible.

2.9. Swift appointment of the members of the PCLOB and release of the PCLOB report on PPD-28

As an independent agency within the executive branch, the PCLOB has an important function with respect to the protection of privacy and civil liberties in the field of counterterrorism policies and their implementation. The Commission recommends the swift appointment of the missing members of the PCLOB by the U.S. administration, so that the PCLOB is able to fulfil all aspects of this function.

Moreover, given the relevance of PPD-28 for the limitations and safeguards applying to government access for signals intelligence, and thus for the Commission's periodic review of its adequacy assessment, the Commission calls on the U.S. administration to publicly release the PCLOB's report on the implementation of PPD-28.

2.10. More timely and comprehensive reporting of relevant developments by U.S. authorities

The Commission recommends that the U.S. authorities proactively fulfil their commitment to provide the Commission with timely and comprehensive information about any developments that could be of relevance for the Privacy Shield, including on developments that are liable to raise questions about the protections afforded under the framework.