Report on the first Swiss–US Privacy Shield Review (2018)

I. Introduction

The Swiss–US Privacy Shield Framework provides for regular annual reviews of the functioning of the Framework (Joint Review Mechanism). Following the entry into force of the Privacy Shield agreement on 17 April 2017, the first Joint Review conducted by the Swiss delegation and the US Government was held in Brussels on 20 October 2018.

Up to now, 2,883 US companies have joined the Swiss–US Privacy Shield programme, including Facebook, Inc., Microsoft Corporation with 27 subsidiaries (covered entities) and Google LLC (last updated: February 2019).

With respect to the commercial part of the Swiss–US Privacy Shield, two cases concerning false claims (companies which falsely claim to be certified under the Privacy Shield) were submitted to the FDPIC in the year under review. Both claims have been resolved in cooperation with the Department of Commerce (DoC) (cf. also point 1.4).

In addition, about ten legitimate complaints against certified companies have been filed with private, independent Alternative Dispute Resolution bodies (ADR). Neither were any complaints filed concerning certified companies that have chosen the FDPIC as an independent appeal body, or concerning employee data (compulsory supervision by the FDPIC).

Furthermore, no case relating to authorities' access to personal data (Ombudsperson mechanism) has been submitted to the FDPIC.

One might conclude that the legal instruments made available by the Swiss–US Privacy Shield have probably been little used so far. It should be noted, however, that the Swiss–US Privacy Shield has only been in force since April 2017. Furthermore it should be borne in mind that any ADR should be preceded by an approach to the certified company itself. It can therefore be assumed that an indeterminate number of violations have already been remedied via direct contact between the individuals and the companies.

Switzerland was represented at the first review by SECO (lead) and the FDPIC (supervisory aspects). The US side included representatives of the DoC.

The meeting took place following the second joint review of the EU–US Privacy Shield, at which the Swiss delegation was present as observers, but was not allowed to ask any questions. Representatives of the following authorities took part in the 2018 EU–US Joint Review on behalf of the US:

- Department of Commerce (DoC),
- Department of State (DoS),
- Federal Trade Commission (FTC),
- Departement of Transportation (DoT),
- Office of the Director of National Intelligence (ODNI),
- Department of Justice (DoJ),
- Privacy and Civil Liberites Oversight Board (PCLOB),
- Temporary acting Ombudsperson (and employee),

- Inspector General of the Intelligence Community

Representatives of the following bodies participated in the review on behalf of the EU:

- European Commission
- European Data Protection Board (EDPB)

The starting points and the text of the Swiss and the EU Privacy Shields are virtually identical. Most of the issues were dealt with exclusively during the EU–US review, including the authorities' access to personal data and various issues regarding the commercial aspects of the Framework (z.B. definition of HR data, field of activities overseen by the FTC/ DoT).

The function of the FDPIC corresponds largely to that of the EDPB (until 25 May 2018: Article 29 Working Party [WP29]).

The EDPB's main findings result from a prior written exchange with the US and discussions during the second EU–US Joint Review. In many cases, they can be adopted analogously for the Swiss–US Privacy Shield Review. In view of the fact that Switzerland and the EU mutually recognise their legal systems as equivalent with regard to data protection, Switzerland confirms the adequate protection of personal data by the Swiss–US Privacy Shield where the EU considers the the protection provided by the EU–US Privacy Shield to be adequate.

At EU level, both the Commision and the EDPB have produced their own reports on both previous joint reviews (2017 and 2018).[1]

For a coordinated procedure, the FDPIC and the EU's data protection authorities were in contact concerning the preparation and follow up of the review. Consequently, the following report overlaps to a large extent with the EDPB's report.

Specific to the Swiss–US Privacy Shield, it is to be noted that personal contact was established with the DoC as part of this first joint review. Furthermore, the procedure for the five officially appointed Swiss–US Privacy Shield arbitrators living in Switzerland, who supplement the EU list, was finalised before the first Swiss–US review. The names of the five additional arbitrators were listed on the International Centre for Dispute Resolution of the American Arbitration Association (ICDR/AAA) above those appointed by the EU. The arbitration mechanism for the Swiss–US Privacy Shield is therefore fully operational.[2]

In addition, the first Swiss–US Privacy Shield Review discussed the establishment and operation of the elements assured in the Swiss–US Privacy Shield Framework, as well as their functioning and development. Switzerland could benefit from the fact that the EU and the US had already conducted a first review of the EU–US Privacy Shield (in force since 12 July 2016). Various recommendations made by the EU as part of its 2017 review were also implemented by the US authorities for the Swiss–US Privacy Shield.

---

[1] https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

[2] cf. also the FDPIC's website which includes a guide to the Swiss-US Privacy Shield: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

With regard to the commercial aspects, the DoC has responded, among other things, to the request of the EU Commission to search more actively for companies that falsely claim to be certified for the Privacy Shield programme.
In addition, it checks certified companies more regularly than at the outset in order to identify potential deficiencies in compliance with the principles.

With regard to official access to personal data by US authorities, the representatives of the EDPB highlighted in the 2018 EU–US review that since the 2017 EU–US review, the US authorities had published documents that contribute to a better understanding of the data collections. The discussion that took place at the second EU–US Review also contributed to a better understanding of the monitoring programmes and to increased transparency (for example, regarding decisions that affect the Foreign Intelligence Surveillance Court [FISA Court]).

From a supervisory point of view, the following remarks are also particularly relevant:

II. Examination of data protection legislation

1. Commercial aspects

1.1. Information and Guidance for US Companies

The understanding of data protection in Switzerland and Europe differs fundamentally from that in the US To prevent any differences of interpretation of the principles laid down in the Privacy Shield, these must be defined in a clear and unambiguous manner. In the self-certification procedure, most US companies conduct a self-assessment and do not use the services of another company for an external compliance review. The procedures to be followed are complex; in particular, the rules on onward transfers of data by certified companies to third parties appear to pose major challenges for companies. In the course of 2018, the FDPIC received a few enquiries regarding this issue because of various ambiguities from Swiss companies which had transferred data to the US In its first review in 2017, the EU called for clear guidance and understandable information to be made available to companies. Thus, the DoC has published FAQs on the 'Accountability for Onward Transfer Principle' on its website.[3] Further instructions are expected.

1.2. Clear and easily accessible Information for Swiss Individuals

Due to the complexity of the Privacy Shield Framework, it may be difficult for Swiss (and European) data subjects to assert their rights. It is therefore necessary that clear, understandable and easily accessible information is available. On its Privacy Shield website, the DoC has posted a webpage (EU and Swiss Individuals) to provide information for data subjects and an overview of the programme.[4] [5]

Further information on the rights of Swiss data subjects is available on the FDPIC website.[6]

[3] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs
https://www.privacyshield.gov/article?id=Processing-FAQs
[4] https://www.privacyshield.gov/Individuals-in-Europe
[5] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq
[6] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

1.3. Self-certification and Re-Certification

Since US companies adhere to the Privacy Shield programme through self-certification and, as mentioned above, only few companies resort to an outside compliance review by a third party, it is important that compliance with the privacy principles is monitored by the DoC during the certification and recertification processes. In this respect, the US authorities have made improvements since the adoption of the Privacy Shield. The DoC now checks the following points for both initial certification and re-certification:

1. Registration with an Independent Recourse Mechanism (IRM) company
2. Payment of fees mentioned in Annex I Arbitral Fund Contribution
3. Compliance with the Privacy Shield Supplemental Principle 6 (access)
4. Completeness and consistency of the certification information
5. Privacy notices (existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policies)

If necessary, the DoC requests the companies to specify the information that can be accessed via the links. In addition, the DoC checks the applications for inconsistencies between the information in the companies' privacy policies and the Privacy Shield list (e.g. information on certification for HR/non HR Data).

According to the information provided by the DoC at the EU–US review, several companies were actually rejected due to non-compliance with the principles on the basis of these reviews.

A notable improvement is the DoC's ban on US companies from referring to the Privacy Shield programme in their privacy policies before the DoC review of the self-certification process has been completed and the company's name has been published on the Privacy Shield lists. Any premature references of the participation in the Privacy Shield program must be removed from the website. As a result, inconsistencies between the information in privacy policies and the actual status of the initial certifications can be avoided.

The re-certification process was also discussed at the EU-US Review. In several cases, the due date displayed on the Privacy Shield list expired before the recertification process was completed and the companies concerned were listed as active Privacy Shield participants for some time without valid certification. The FDPIC joins the EDPB's opinion that, as long as the US companies still publicly commit to apply the Privacy Shield Principles there is no gap in the protection of individuals. However it would be desirable to completely rule out uncertainties as to whether a US fully commits itself to the programme.

1.4. Oversight and Supervision of Compliance with the Principles by the DoC

The second EU-US review revealed significant improvements by the US authorities regarding the oversight of the compliance of certified companies with the principles. The DoC carries out official ckecks, such as:

- Quarterly, it identifies false claims (companies that falsely claim to be certified as Privacy Shield).

So far, the FDPIC has received two cases of false claims, both of which have been resolved in cooperation with the DoC.

- The DoC will send a letter to the companies identified as "non-compliant", warning them of potential transmission to the FTC/DoT in the event of continued non-compliance with the requirements or failure to delete entry as a Privay Shield participant. Companies have 30 days to respond. The DoC maintains a list of companies that do not respond to the letter.

- The DoC also carries out random web searches.

- The DoC has performed a sweep of randomly sampled 100 companies (including EU-US Privacy Shield). The focus was on access to the privacy policies, the companies' willingness to react and the availability of the IRM.

- One person is responsible for searching the media for keywords in order to identify possible violations of the Privacy Shield Framework.

- The DoC regularly checks companies for broken links to the Privacy Policy on the Privacy Shield list.

In the context of the second EU-US joint review, the EDPB welcomed the addition of these new surveillance measures, but regretted that the same were limited to formalities. Substantive reviews, however, are crucial. It is important to review all principles, in particular or onward transfers. For example, the DoC had not yet requested any copies of the privacy provisions from contracts between US organisations and their agents. However, since onward transfers can also be made in third countries without adequate data protection, there should be clarity regarding the accountability. In the DoC's view, however, the Privacy Shield does not include reviews at such a high level of detail.

During the first Swiss–US review, the DoC expressed to the FDPIC that, in its opinion, the Privacy Shield framework is comparable to a law text that is binding for the certified companies, but that data subjects must (also) take action themselves to enforce their rights. Accordingly, the DoC usually conducts investigations at US companies upon external notification.

The FDPIC agrees with the EDPB. It considers ex officio supervision by the US authorities to be appropriate, in particular since due to the complexity of the data processing, which might not always be obvious for data subjects, it may be difficult for the latter to actually assert their rights.

1.5. Oversight and Supervision of Compliance with the Principles by the FTC

At its first joint review, the FDPIC did not have the opportunity to establish direct contact with representatives of the FTC, since the latter took part exclusively in the EU–US review. However, the statements made there also apply analogously to the Swiss–US Privacy Shield agreement.

Since last year's EU–US review, the FTC has increased its activities regarding the oversight and enforcement of the Privacy Shield Principles.

According to the FTC, a total of 40 lawyers are now working almost exclusively on privacy issues, with additional support from technical experts, among others.

The FTC recorded several new cases of non-compliance with the Privacy Shield Principles; however it is beyond the FDPIC's knowledge whether any cases amongst those were related to the Swiss-US Privacy Shield.

The FTC sent civil investigation demands (CIDs), on an experimental basis, to monitor compliance with the Privacy Shield Principles. It did not, however, disclose any details of the target objects and content of the forms. In general the FTC seems to have a broad discretion to do sweeps. There is no need for the FTC to demonstrate that it has a reasonable suspicion.

The FDPIC as well as the EDPB welcome the ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. However, since the FTC has not provided any details, it is not possible to assess the specific cases and the activities of the FTC, nor to assess the extent to which the FTC actually verifies compliance with the principles.

1.6. Independent Recourse Mechanisms

The DoC has issued guidelines for harmonising the annual reports of companies offering IRM services and making the content of these reports clearer. These guidelines also emphasize potential conflicts of interest for companies that offer both ex officio compliance and IRM services to the same US companies. Such companies are asked to describe in their annual reports how they intend to avoid such conflicts of interest.

1.7 HR data

There is a discrepancy in the interpretation of the term 'HR data' (DE: Personaldaten) by the US authorities on the one hand and the Swiss and EU representatives on the other hand. The subject was discussed already at the first 2017 EU–US Review as well as in the subsequent WP29 report. According to the understanding of the US authorites, only employee data that are transferred to the US within the same company fall within the category of HR data. Employee data from a Swiss (or EU) company that are being transferred to a Privacy Shield certified processor within the US are not considered HR data but commercial data. Consequently, such data do not benefit from the enhanced/additional protection provided by the Privacy Shield Framework for HR data (such as being subject to FDPIC authority, which can make binding recommendations to US companies).

The FDPIC agrees with the WP29 (and the EDPB) that the term HR data should include any personal data processed in the EU or Switzerland in the context of an employment relationship, whether processed by the employer or by a processor. HR data may therefore only be transferred lawfully to a US company under the Privacy Shield if the receiving company has an active HR data certification. The FDPIC considers that all data concerning an employee that are collected in Switzerland need special protection: Due to the subordination relationship in data collection, employees are not entirely free to disclose their personal data. It is therefore important that personal data are subject to the enhanced protection provided for further processing (e.g. the express consent to opt in instead of opting out from the processing of their data for marketing purposes).

The disagreements regarding these interpretations have not yet been resolved by the EU and US authorities. After the definition of HR data was discussed at the last EU–US review, this year's review focused on the consequences of the different interpretations. The EU representatives expressed particular concerns that the more restrictive rules for the protection of workers promised in the Privacy Shield agreement could not be enforced. At the Swiss review, the FDPIC explained to the DoC that it fully agreed with the EDPB's view.

2. Authorities' Access to Personal Data / National Security

The US representatives responsible for national security attended the EU–US review only. In view of the fact that the EU and Switzerland mutually guarantee adequate data protection, the FDPIC can endorse the observations made on authorities' access in the analyses by the EDBP, referring to the EDBP report of 22 January 2019 and the WP29 report of 28 November 2017[7].

2.1. Data Collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12 333

In particular, the EDPB requires independent assessments of whether data collections under Section 702 FISA are indiscriminate and mass surveillence takes place.

The EDPB maintains the statements made in the WP29 report of 28 November 2017, in particular that, with regard to proportionality in general and necessity in particular, it demads independent assessments of the definition of the term "target" and of the "tasking of selectors" (e.g. telephone, e-mail address, etc.).

The EDBP regrets that the reauthorisation of Section 702 FISA at the end of 2017 did not include the implementation of additional safeguards to protect EU (resp. Swiss) data subjects, e.g. in accordance with the PPD-28. The PPD-28 stipulates, among other things, that data collection should be 'as tailored and as feasible as possible'. It also stipulates some safeguards for the protection of personal information pertaining to any private individual irrespective of their nationality or their place of residence. The use of personal data obtained through mass surveillance is limited to six purposes.

With regard to surveillance in which (based on EO 12 333) personal data is collected outside the US, the EDBP refers to the observations of the WP29 in the context of the first EU–US review. According to the EDBP, in order to guarantee an adequate level of data protection in a third country, not only data processing within that country's physical borders should be appropriate, but also 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. This must also apply to Swiss personal data.

According to the US authorities on the other hand, EO 12 333 could not be used as a basis for collection of data inside the US territory. They consider that collection of data under EO 12 333 falls outside the scope of the Privacy Shield.

The EDBP welcomed the general application of PPD-28 confirmed by the US authorities.

[7] https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf

However, after analysing the information on PPD-28 provided by the US authorities, the EDBP came to the conclusion that neither the PCLOB report on PPD-28 nor the second EU–US review provided substancial new information on the application of the PPD-28 text. In particular, it mentions ambiguities in the interpretation of the six purposes above. In addition, the EDBP would welcome a detailed follow-up report on the application of PPD-28 for the various surveillance programmes. It is, moreover, desireable for the the PCLOB to provide information in its report on EO 12 333, which has still to be completed, on the concrete applicability of PPD-28 and on the necessity and proportionality of the data collections based on this directive.

2.2. Oversight by US Authorities of the Surveillance Programmes

The EDBP draws attention to the importance of oversight by the US authorities of the surveillance programmes. The oversight activities of various U.S institutions were already explained at the 2017 EU–US Review. Additional presentations were made at the second EU.US review, which confirmed the EDPBs understanding of the Inspector General community.

The EDBP considers the responsible oversight bodies to be independent from the Intelligence Community (including the Privacy and Civil Liberty officers, the oversight of the Department of Justice and Inspector Generals).

The EDBP considers the PCLOB as an essential element in the framework providing oversight over the US authorities. Following the WP29's request in first review of the EU–US Privacy Shield to fill the four remaining seats on the PCLOB, the US Senate confirmed three members, including new chairman Adam Klein on 11 October 2018, fulfilling the conditions for the PCLOB to constitute a quorum. Thus, the PCLOB can perform its duties as an independent supervisory body. The vacancies remain to be filled.

2.3. Legal Recourse for Swiss Data Subjects

In the Schrems judgment relevant to the EU–US Privacy Shield (and indirectly to the Swiss–US Privacy Shield), the Court of Justice of the European Union (CJEU) stated that, under Article 47 of the Charter of Fundamental Rights of the European Union, data subjects must have the right of recourse in a national court. This means that provision should be made to offer individuals legal remedies that allow them to access their personal data in order to rectify or delete them.

The Swiss Federal Constitution also guarantees proceedings before an independent and impartial tribunal (Art. 29ff). A third country whose data protection is to be regarded as adequate must also provide a court before which an effective appeal can be lodged.

The PPD-28 does not create enforceable rights. Illegal electronic surveillance based on EO 12 333 does not offer any redress mechanism either.
Due to the restrictive interpretation of the "standing requirement", FISA appears to provide limited grounds for Swiss (or EU) individuals to challenge surveillance in US courts. The United States Supreme Court does not consider the abstract risk of surveillance sufficient to warrant judicial review; it requires proof of surveillance of communications.

It is extremely difficult for Swiss (or EU) data subjects to challenge surveillance measures before a court or to have them reviewed. This is problematic in view of the fundamental right

to effective judicial protection. Further developments regarding the interpretation of the standing requirement in the area of surveillance will be followed (including in pending cases).[8]

Due to the unlikeliness to seek effective redress before a US court in surveillance matters, the Ombudsperson mechanism is currently practically the only (direct) possibility for Swiss data subjects to verify compliance with data protection principles (PPD-28, EO 12 333, FISA Section 702, etc.) by US authorities. Thus, the procedural principles of this Ombudspersonmechanism must be subject to high standards. These are analysed below.

2.4 Ombudspersonmechanism

Access to the Ombudsperson procedure was implemented in the first year after the Swiss–US Privacy Shield came into force. The EDPB as well as the FDPIC welcome the establishment of an Ombudsperson mechanism as a new redress mechanism. The Ombudsperson examines requests and in the event of a violation of privacy, refers the matter to the competent Inspector General to check the internal policies of these authorities.

The procedural guarantees of the Swiss Federal Constitution place high demands on the independence and impartiality of the Ombudsperson.

A new acting Ombudsperson, Manisha Sing (Acting Under Secretary of State for Economic Growth, Energy, and the Environment), was appointed on 28 September 2018. She replaced Judith Garber (Acting Assistant Secretary for Oceans, Environment and Science at the Department of State).

At the second Joint Review des EU–US Privacy Shield, the Ombudsperson and other representatives of the US Administration explained the functioning of the mechanism on the basis of a theoretical case. They underlined that the Ombudsperson was independent from the US intelligence services and and would process enquiries from data subjects relating to infringements of the data protection principles lawfully and efficiently. The Ombudsperson would in any event respond to enquiries from data subjects only after she is convinced that there is no data breach. In order to ensure compliance, the Ombudsperson may use the presidentially mandated power to **escalate requests** to highest level, including the Secretary of State. According to the Ombudsperson, specific cases may not, however, be made public, and the actual procedure in individual cases and the interaction between the Ombudsperson and the intelligence community in the United States are partially classified. As long as these processes are not disclosed, it is not possible to conclusively assess the Ombudsperson's actual powers vis-à-vis the intelligence community, i.e., whether the Ombudsperson has sufficient powers to obtain the information required and address shortcomings.

Therefore, it is currently doubtful whether sufficient remedial action can actually be taken in the event of non-compliance with the privacy principles by US authorities. This proves to be problematic with regard to the constitutional guarantees for a hearing before an independent and impartial court, especially since the EU–US review confirmed that the decisions of the Ombudsperson can not be brought before a court.

[8] See also EDSA report of 22 January 2019, Section. 4.4. p. 18, in particular, also the cases ACLU v/ Clapper and Wikipedia v/ NSA

In addition, the position of Under Secretary, to whom the office of Ombudsperson is assigned, is not yet filled on a permanent basis. It is therefore necessary to appoint a permanent Ombudsperson.

In January 2019, President Donald Trump nominated Keith Krach as Under Secretary of State for Economic Growth, Energy and the Environment. According to the wording of the Privacy Shield Framework, he would be appointed as the permanent Ombudsperson. The FDPIC will follow up subsequent developments. The confirmation by the Senat is currently pending.

2.5 Access to Personal Data by Law Enforcement Authorities

The FDPIC notes that the rights of third country nationals are subject to certain restrictions under US criminal procedural law with regard to ex-post notifications of third-party data collections. These restrictions may also have a negative effect on data subjects with Swiss citizenship.

III. Conclusion:

The FDPIC welcomes the implementation of the elements of the Swiss–US Privacy Shield Framework during the first year and of various improvements (required by the EU before and during the first review) which have also been implemented for the Swiss–US Privacy Shield Framework. These include for example adjustments to the certification process, a more detailed review by the US authorities on their own initiative and the publication/making available of various helpful documents. It is also positive that three seats on the PCLOB have been filled, thus achieving the required quorum.

Another positive development is the appointment of five arbitrators for Switzerland, which supplement the list of EU arbitrators.

There are, however, several areas which should be improved.

For example, it would be worth considering having the US authorities conduct substantial reviews of Privacy Shield-certified US companies.

The FDPIC will also follow the further discussions between the EU Commission and the US authorities on the definition of the term ‘HR data’.

With regard to access to personal data by US authorities, it is important, as the EDBP noted in its report of 22 January 2019, that the PCLOB, in its capacity as the oversight board, produces further reports, in particular on the application of the protection measures under PPD-28, and reports relating to Section 702 FISA and EO 12 333.

Furthermore, a permanent Ombudsperson should be appointed.

The EDBP also refers to the relevant cases pending before the European Court of Justice (EUCJ), for example relating to standard clauses in contracts, which must be awaited and which will have indirect effects on Switzerland.