Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner
FDPIC

Report on the second Swiss-US Privacy Shield review (2019)

I. Overview

The second annual joint review of the Swiss-US Privacy Shield conducted by the Swiss delegation and the US Government was held in Washington D.C. on 14 September 2019.

Since the Swiss-US Privacy Shield framework entered into force on 17 April 2017, more than 3,300 organisations have joined the programme; since the last review in October 2018, there have been almost 1,000 new certifications. Over 70% of members are SMEs from various sectors, particularly information and communications technology, corporate and professional services, media and entertainment, and education. Corporations such as Facebook Inc. and Google LLC are also still Privacy Shield certified.

The Federal Data Protection and Information Commissioner (FDPIC) is the point of contact for data subjects and organisations in Switzerland.

With respect to the commercial part of the Swiss-US Privacy Shield, only one case was submitted to the FDPIC to be forwarded to the US Department of Commerce (DoC) in the year under review. The case concerned a false claim (organisations which falsely claim to be Privacy Shield certified). The case was resolved in cooperation with the Department of Commerce (cf. also section 1.4 below).

In addition, around ten legitimate complaints against certified organisations in relation to the Swiss-US Privacy Shield framework were filed with private, independent Alternative Dispute Resolution bodies (ADR). No complaints were filed concerning certified organisations that have chosen the FDPIC as an independent appeal body, or concerning employee data (mandatory supervision by the FDPIC). On the other hand, the FDPIC was consulted several times by organisations based in Switzerland regarding ambiguities in data transfer with the United States.

No cases regarding US authorities' access to personal data for national security purposes have been submitted to the FDPIC since the framework was implemented.

As before, it is difficult to assess why little use is made of the available legal instruments by data subjects in Switzerland. This may be due to the complexity of the framework and the difficulty in detecting data breaches. As has already been stated, if data subjects or organisations in Switzerland have questions, they can contact the FDPIC. It should however be noted that before contacting an ADR or the FDPIC, parties should first approach the certified organisation itself. It should therefore be assumed that a number of data breaches – on which it is difficult to put a precise figure – could be resolved this way.

As in the previous year, Switzerland was represented in the second review by SECO (lead) and the FDPIC (data protection/supervisory aspects). The US side was represented by members of the DoC.

The meeting took place following the third joint review of the EU-US Privacy Shield, at which the Swiss delegation was present as an observer but was not permitted to play an active role. Representatives of the following US authorities took part in the 2019 EU-US joint review:

- Department of Commerce (DoC),
- Department of State (DoS),
- Federal Trade Commission (FTC),
- Department of Transportation (DoT),

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

- Office of the Director of National Intelligence (ODNI),
- Department of Justice (DoJ),
- Privacy and Civil Liberties Oversight Board (PCLOB, independent body for monitoring the protection of privacy and civil liberties),
- Ombudsperson (and employees),
- Inspector General of the Intelligence Community

Representatives of the following EU bodies participated in the review:

- European Commission
- Eight representatives of the European Data Protection Board (EDPB)

As in the previous year, given that the content of the Swiss and EU frameworks corresponds in virtually all respects, most issues – such as authorities' access to personal data and key data protection aspects of the commercial part (e.g. FTC/DoT activities) – were dealt with exclusively in the EU-US review (cf. also FDPIC report on the first joint Privacy Shield review, 2018).

At EU level, both the Commission and the EDPB (until 25 May 2018: Article 29 Working Party [WP29]) have produced their own reports on all previous joint reviews (2017 , 2018 and 2019).

The EDPB's main data protection findings result from a prior written exchange with the US, and discussions during the third EU-US joint review. They generally apply by analogy to the Swiss-US Privacy Shield. The US authorities then carry out their modifications to both frameworks on this common basis.

The FDPIC's role corresponds largely to that of the EDPB (formerly WP29).

Consequently, this report overlaps to a large extent with that of the EDPB.

In view of the fact that Switzerland and the EU mutually recognise their legal systems as equivalent with regard to data protection, Switzerland accepts that protection of personal data by the Swiss-US Privacy Shield is adequate where the EU considers the protection provided by the EU-US Privacy Shield to be adequate.

After the first review of the Swiss-US Privacy Shield framework (in 2018) focused on establishment and flow of processes in the commercial part of the Privacy Shield programme and on establishing personal contact with the US representatives, this year there were also intensive discussions on use of the Privacy Shield framework by organisations based in Switzerland and on specific adjustments and developments to the commercial part.

In the interests of completeness, it should be mentioned that an arbitrator living in Switzerland had his name removed from the list during the year under review. The US authorities decided not to replace him for the time being. Nonetheless, the arbitration mechanism for the Swiss-US Privacy Shield remains fully operational.

From a data protection point of view, the following points are also particularly relevant:

II. Examination of data protection legislation

1. Commercial aspects

1.1. Information and guidance for US organisations

As the level of data protection in the United States is not deemed equivalent to that in Switzerland, data transfer from Switzerland to the United States is in principle only allowed under the conditions set out in Art. 6 of the Federal Data Protection Act (SR 235.1, FADP). The Privacy Shield framework is therefore designed to guarantee an adequate level of data protection to make it easier for certified organisations to transfer data to the United States within the scope of the Privacy Shield text. On account of this and due to the fact that the understanding of data protection in the US differs fundamentally from that in Switzerland (and the EU), ensuring uniform interpretation of the Privacy Shield text is of paramount importance.

On account of this and at the request of the WB29 and the EDPB (cf. their reports), since the Privacy Shield framework was implemented the DoC has provided accessible and readily understandable guidelines for certified organisations in the form of FAQs (e.g. Accountability for Onward Transfer Principle, Processing Guidance).

Last year, the DoC also published an FAQs factsheet on the Privacy Shield and the United Kingdom (Brexit).

The FDPIC welcomes the DoC's proactive approach to helping organisations and interested parties understand the complex Privacy Shield text.

Having received several requests from organisations based in Switzerland, the FDPIC supports the EDPB's proposal that the DoC should explain in more detail, among other things, the procedure for contract data processing and the use of standard contractual clauses (SCCs).

1.2. Clear and easily accessible information for Swiss data subjects

As mentioned under section 1, the complexity of the Privacy Shield framework may mean it is difficult for Swiss (and European) data subjects to assert their rights. At the request of the WP29 and later of the EDPB (cf. their reports), during the first years of application of the EU-US and Swiss-US Privacy Shields the US authorities published on their website more easily understandable information on the rights of subjects, the available resources and the redress mechanisms. The different ways of filing complaints are also now explained and, in some cases, relevant links are provided. Following the first annual reviews of the framework and in response to the WP29 proposals, the DoC added a one-page document to its website that provides an overview of the programme, focusing on the rights of data subjects and how they can be exercised.

Further guidelines are expected.

Further information on the rights of Swiss data subjects is available on the FDPIC website. As mentioned above, the FDPIC can be consulted in writing or by phone if there are issues that require clarification.

1.3. Self-certification and recertification

Regarding initial certification and recertification, there were no changes in the DoC's review of organisations' compliance with the Privacy Shield principles compared to last year's joint review. The DoC still checks the following points for both initial certification and recertification:

1. Registration with an Independent Recourse Mechanism (IRM) company
2. Payment of fee mentioned in Annex I Arbitral Fund Contribution
3. Compliance with the Privacy Shield Supplemental Principle 8 (access to personal data)
4. Completeness and consistency of the certification information
5. Privacy notices (existence in the organisations' privacy policies of all 13 elements required by the Privacy Shield is also checked)

As before, where necessary the DoC requires organisations to specify the information that can be accessed via the links to make it easier for data subjects to assert their rights. In addition, the DoC checks applications for inconsistencies between the information in the organisations' privacy policies and that on the Privacy Shield list (e.g. information on certification for HR/non HR data). Once again, these checks allowed the DoC to identify several cases of non-compliance with the requirements, and to exclude from membership companies that did not comply with the Privacy Shield.

The DoC still prohibits US organisations 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 organisation's name has been published on the Privacy Shield lists in order to avoid inconsistencies between the information in privacy policies and the actual status of the initial certifications.

The FDPIC considers these measures to be of great value. However, both the EDPB and the FDPIC continue to view as problematic the fact that the tests conducted by the DoC in accordance with the information received in the review relate primarily to formal criteria rather than respect of the actual Privacy Shield principles.

Such a substantive check would be advisable, however, particularly as most organisations conduct their own compliance assessment rather than having this carried out by a third party.

As in last year's EU-US Privacy Shield Review, an issue relating to recertification was discussed, namely that in some cases the validity date of initial certification expired before the completion of the recertification process, leaving some companies listed as active for some time despite not having valid certification. According to information provided in the EU-US Privacy Shield Review, the recertification process may take up to 105 days from the expiry of the validity period. Throughout this time, companies are still listed as active.

The FDPIC agrees with the EDPB that as long as the US organisations still publicly commit to applying the Privacy Shield principles, individuals are not disadvantaged in any way. However, the FDPIC also agrees with the EDPB that it would be desirable to find a solution that guarantees the protection of data subjects at all times and rules out any uncertainties. In the meantime, both data subjects and organisations in Switzerland and the EU that transfer personal data to certified US organisations should be made aware that they always need to check whether the organisation's certification is valid.

During the third EU-US Privacy Shield review it was also discovered that there were several organisations listed as active on the Privacy Shield list whose recertification was due in 2018. The EDPB called on the DoC during this year's review to introduce processes to ensure that the list of active participants is always up to date.

1.4. Oversight and supervision of compliance with the principles – DoC activities

In the first EU-US Privacy Shield review report (2017), the WP29 criticised the fact that 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 ex officio oversight and supervision of compliance.

In the subsequent Privacy Shield review in 2018 (the first for the Swiss-US Privacy Shield), significant improvements in oversight by the US authorities were noted concerning both frameworks (cf. FDPIC 2018 report, section 1.4).

According to this year's information, the DoC last year increased the number of spot checks of randomly chosen organisations to 30 per month, and issued more than 670 warnings, most of them regarding false claims. While these steps taken by the DoC to ensure formal compliance with the Privacy Shield principles are to be welcomed, as stated in the last report, the EDPB and the FDPIC are concerned that these checks still remain focused on the formalities to be complied with rather than on whether the substance of the principles is observed. The EDPB would therefore still urge the DoB, in the third review, to extend its oversight activities to substantive elements, such as the purpose limitation principle. In the context of onward transfers, too, the DoC has still not made use of its right to request a copy of the relevant privacy provisions in contracts between US organisations and their agents. Since onward transfers may lead to transfers to third countries which may not have adequate data protection, accountability must be monitored.

The DoC maintains its view that, when certifying with the Privacy Shield, companies enter into legally enforceable obligations. The individuals must also take action themselves to enforce their rights. It also points out that the framework does not provide for more substantive controls (see also Section 1.4 p. 5 of the 2018 report). However, spot checks could be extended to cover more aspects.

Like the EDPB, the FDPIC also feels that substantive reviews could be carried out by the DoC to check that self-certified organisations are specifically implementing the substantive requirements of the Privacy Shield. The FDPIC will monitor developments and remain in contact with representatives from the EU and United States.

1.5. Oversight and supervision of compliance with the principles – FTC activities

During the second joint review, the FDPIC once again did not have the opportunity to establish direct contact with FTC representatives as the latter only took part in the EU-US review, in which Switzerland was merely an observer and so was not permitted to ask any questions (cf. section 1). However, the statements made there also apply by analogy to the Swiss-US Privacy Shield framework.

Since the last Privacy Shield review, the FTC has recorded a total of seven new cases. Instances of non-compliance concerned administrative errors rather than a substantive breach of the Privacy Shield principles. The EDPB recommends conducting further checks concerning onward transfers, given that the solutions put in place by organisations are not checked by the DoC either.

In the FTC Division of Privacy and Identity Protection, Bureau of Consumer Protection, there are 40 lawyers working almost exclusively on the topic of data privacy. They are supported by various people, including technical experts. The FTC clarified in this year's review that the Facebook settlement reached last year remains outside the scope of the Privacy Shield.

The EDPB welcomed the increased ex-officio activity undertaken by the FTC. But as the FTC does not provide any details, it is still not possible to assess the individual cases and the activities undertaken by

the FTC. It is thus impossible to gauge to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.

1.6. Independent Recourse Mechanisms (IRM)

The number of complaints received by IRM providers has risen slightly since the last review. However, the complaints appear to mainly concern procedural aspects and not substantive compliance with the principles. The IRM mechanism cannot therefore replace enhanced substantive checks by the US authorities (cf. sections 1.4 and 1.5).

As stated in the report on the 2018 review, companies that offer IRM are required to describe in their annual reports how they intend to avoid or resolve conflicts of interest (cf. section 1.6, p.6 of the 2018 report). On this point, the DoC remarked that it has updated its guidelines for the annual IRM report in order to highlight potential conflicts of interest by including a description of how such situations can be avoided. The guidelines do not cover all aspects of the reports, however. In particular, the EDPB found that no standardised template format for the reports has been introduced yet on this aspect. To ensure full comparability, the EDPB thus advises the DoC to introduce a standardised template format for the IRM report which also includes explanations of how potential conflicts of interest can be avoided.

1.7 HR data

As already mentioned in the last report (cf. section 1.7, 2018 report), the term 'HR data' in the context of the Privacy Shield is interpreted differently by the EU and Switzerland on the one hand and the US authorities on the other. The DoC and the EU authorities continued discussions on the different interpretations of HR data last year but failed to come to an agreement. On account of this unresolved discrepancy in definitions, the focus in both the last and this review was less on the term and more on the possible implications of the different definitions. The EDPB and the FDPIC fear that the additional protection measures stipulated in the framework for HR data (e.g. opt-in rather than opt-out for marketing purposes) would not be enforced by any US or EU authority for non-HR data. The FDPIC is of the same view as the EDPB that personal data should be subject to more stringent requirements, regardless of whether they are processed by the employer or by a processor (cf. also 2018 report, section 1.7). Discussions between the EU and the US authorities on this matter are continuing.

2. Authorities' access to personal data for national security

The legal framework in the United States has not substantially changed since the last review. The major reservations expressed by the WP29/EDPB and the FDPIC in last year's reports regarding authorities' access to personal data within the scope of the Privacy Shield for the purpose of national security or law enforcement thus remain. The concerns particularly affect data collection, oversight, legal recourse and the ombudsperson mechanism. It should also be noted that the Schrems II case (Case C-311/18), which is still pending before the European Court of Justice (ECJ), also affects the EU-US Privacy Shield and thus has an indirect impact on the Swiss-US Privacy Shield. The judgment is expected in January 2020.

The US representatives responsible for national security only attended the EU-US review, at which the FDPIC was an observer and was not allowed to take part directly. As the frameworks are equivalent, the FDPIC can endorse the observations on authorities' access made by the EDPB, unless explicitly stated otherwise below. Particular reference is thus made to the EDPB report of 12 November 2019, cf. section

1 above and the reports of 22 January 2019 and the WP29 report of 28 November 2017, section I above).

2.1. Data collection for national security purposes

2.1.1 Data collection under Section 702 Foreign Intelligence Surveillance Act (FISA)

The EDPB once again emphasises the need for an independent assessment of the proportionality and necessity regarding the definition of 'targets' and the concept of 'foreign intelligence' under Section 702 FISA (including in the context of the UPSTREAM programme), and maintains its call for further independent assessment of the process of applying selectors in specific cases ('tasking of selectors', e.g. phone, email address etc.). It also continues to call for further clarifications/explanations regarding the UPSTREAM surveillance programme to prevent massive and indiscriminate access to the personal data of non-US persons (cf. 2018 report, section 2.1).

With regard to Section 702 FISA, it was established during the discussions of this year's review that a 'person' to be identified as a target could refer to several individuals using the same identifier, where all these individuals were non-US persons and fulfilled the applicable criteria for being targeted.

The EDPB welcomes the fact that the now fully functional Privacy and Civil Liberties Oversight Board (PCLOB) as an independent oversight agency has decided "to review the FBI's querying (search) of data obtained pursuant to Section 702" as well as the fact that the PCLOB has indicated it is following up on how the previous recommendations set out in its report on Section 702 were taken into account. However, the EDPB regrets that the PCLOB does not intend to prepare and issue an updated general report on Section 702, building on the report issued in 2014. A general updated report would help provide an assessment of the new provisions in Section 702 (reauthorised in 2017), as well as on the practice of intelligence agencies.

2.1.2. Data collection under the Executive Order 12333 (EO 12333)

The EDPB maintains the position that any assessment of the adequacy of data protection in a third country should not be limited to the extent of surveillance within its physical/geographical borders. Instead, it should include an analysis of the legal basis on which the country can conduct surveillance outside its territory with regard to EU (and Swiss) data. Limitations to governmental access to personal data should extend to data 'on its way' to the country for which adequacy is recognised.

During the last review, the US authorities stressed that EO 12333 could not be used as a basis for data collection on US territory, and that data collection under EO 12333 falls outside the scope of the Privacy Shield (cf. also last year's FDPIC report, section 2.1).

Given the continued uncertainty and unforeseeability of how EO 12333 is applied, the EDPB stressed the importance of PCLOB reports to clarify this text. It is to be assumed, however, that any such reports will be kept classified, and that no further information on how EO 12333 functions (and on its necessity and proportionality) will be made available to the public, nor to representatives of third countries.

2.1.3. Protection measures under the Presidential Policy Directive 28 (PPD-28)

The EDPB welcomed the (general) application of PPD-28 confirmed by the US authorities (cf. also FDPIC report on first review, 2018), particularly as it is the only piece of legislation that provides for

guarantees and limitations on the collection and use of data outside of the United States (the limitations of FISA or other more specific US laws do not apply here).

Mass data collection is limited under the PPD-28 to six national security purposes (detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to US or allied armed forces; and combating transnational criminal threats, including sanctions evasion) to better protect the privacy of all individuals, including non-US persons. No new substantive discussions took place in the context of the third EU-US Privacy Shield review concerning the interpretation and application of the six security purposes, which would allow a validation of the assurances provided by the US authorities.

Although the US authorities claim that the Executive Orders and Presidential Policy Directives have the 'force of law', it should be borne in mind that these legal instruments do not confer any enforceable rights. It would therefore not be possible for an EU or Swiss data subject to directly invoke the violation of PPD-28 safeguards before a US court (cf. also FDPIC 2018 report, section 2.3).

2.2. Oversight of US authorities' surveillance programmes

The EDPB points out that comprehensive oversight of all surveillance programmes is crucial.

The oversight activities of several entities were already presented during the two previous annual joint reviews. In the EDPB's view, a comprehensive oversight structure is in place, composed of a range of elements that are in part independent from the intelligence community, including the Privacy and Civil Liberty officers, the Inspector Generals, the PCLOB, the FISC and Congress.

The EDPB welcomes the appointment of the final members of the PCLOB, which is now fully functioning and operational. The PCLOB presented its work programme for the first time, and the EDPB welcomed the transparency provided by this oversight body. The EDPB considers the PCLOB an essential element in the oversight structure.

The EDPB also renewed calls for the publication of reports and the update of previous reports (Section 702 FISA, PPD-28).

In general, it should be noted that it is very difficult to carry out a meaningful review of the oversight of the US authorities's surveillance programmes because representatives of third countries are granted access to official documents only.

2.3. Legal recourse for Swiss data subjects

As mentioned in last year's FDPIC report (section 2.3), for a third country's data protection level to be regarded as adequate, it is crucial that data subjects in Switzerland have access to an independent and impartial appeal body.

As, according to the US authorities, the legal framework has not changed since the last review, we refer to the observations made in the last review (cf. FDPIC 2018 report, section 2.3).

Due to the restrictive interpretation of the 'standing requirements', it remains unrealistic for Swiss (or EU) individuals to challenge surveillance (Section 702 FISA, EO 12333 etc.) in US courts. During the EU-US review it was confirmed that the interpretation of the notion of 'standing' in surveillance matters is evolving with cases still pending.

2.4. Ombudsperson mechanism

In the EU-US Privacy Shield Review, the EDPB welcomed the nomination of Mr Keith Krach as 'permanent' ombudsperson on 18 January 2019.

As the ombudsperson mechanism is currently virtually the only way to monitor compliance of the US authorities with the data protection principles under PPD-28, EO 12333, Section 702 FISA etc., it is crucial for the ombudsperson to be independent and impartial.

As Under Secretary of State for Economic Growth, Energy, and the Environment, Mr Keith Krach is independent from the US intelligence services, but not independent of the US government.

Concerning the handling of requests from data subjects, in previous reviews the ombudspersons and representatives of the US government explained what was done to ensure that requests are handled lawfully and efficiently. Staff of the ombudsperson explained how requests are handled on the basis of a theoretical case (cf. also FDPIC 2018 report, section 2.4). Mr Keith Krach reiterated the statements of the previous ombudsperson that he only signed letters to close cases if he was convinced that they had been dealt with correctly, and that he would escalate requests to the highest level of the US government if he was unconvinced of the outcome presented to him.

The procedures governing the access to relevant information by the ombudsperson and their interactions with the other members of the intelligence community, including the oversight bodies, remain partially classified, which makes it very difficult to assess the procedure.

While there are no specific reasons to doubt the integrity of the new ombudsperson, the EDPB demands more information on their powers vis-à-vis the intelligence community.

On the basis of the available information, it is still not possible to conclusively assess whether the ombudsperson has adequate powers vis-à-vis the intelligence community as in the event of an infringement, their power seems to be limited to deciding not to confirm compliance towards the petitioner. Furthermore, the ombudsperson's decisions cannot be brought before a court.

This is problematic with regard to the constitutional guarantees of a hearing before an independent and impartial court.

III. Conclusion:

The FDPIC welcomes the efforts of the US authorities to improve the Privacy Shield programme, especially the ex officio oversight and implementation measures, as well as the appointment of the remaining members of the PCLOB and the permanent ombudsperson.

There are still some areas that should be improved, however. In terms of commercial aspects, both the EDPB and the FDPIC still have concerns, e.g. on the conduct of substantive reviews by the DoC, compliance with the onward transfer requirements, and resolution of the HR data issues.

In terms of data collection by US authorities, among other things it would be helpful to have reports, for example on the guarantees under PPD-28.

It is still not possible to conclude on the basis of information from the EU-US Review that the ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Nor can it

be said unequivocally that the ombudsperson mechanism for the Swiss-US Privacy Shield meets the requirements of an independent, unbiased appeal authority.

It is worth remembering that the same concerns will be addressed in the cases pending before the European Court of Justice (ECJ) – in particular the Schrems II case, which will also have an indirect effect on Switzerland.