

10. Swiss US Privacy Shield: Registration and Enforcement

Dr. Reinhard Oertli, Meyerlustenberger Lachenal, Zurich



Purpose and Effect

1. Adequate protection

It is crucial for any data protection regime to make sure that its protection objective is not undermined and frustrated by transferring the protected data to another jurisdiction which allows for forms of data processing that would be prohibited in the country of origin. That is why the Swiss Federal Act for Data Protection (FADP) in the same way as the EU General Data Protection Regulation (GDPR) stipulates that specific conditions must be met before any cross-border disclosure of personal data unless the receiving country has "legislation that guarantees adequate protection". Meeting these requirements is cumbersome and hampers the data transfer. Also, the main tools used in such situations, standard data protection clauses and binding corporate rules, can regulate private behavior, but they cannot prevent interference by state authorities or other public bodies without adequate safeguard of private interests.

The US data protection regime has not been considered adequate by the Swiss and the EU authorities, but an unhindered data flow to the USA is of vital importance to the Swiss and the European economy.

2. Privacy Shield Frameworks

Following the conclusion of the new Privacy Shield Framework between the EU and the USA (*EU-US Privacy Shield*) in 2016, a practically identical arrangement was established between Switzerland and the US (*Swiss-US Privacy Shield*) in 2017.

US companies can register under either or both of these frameworks, having the effect that EU and Swiss companies can transfer personal data to them as if they were located in a country with adequate protection standards.

3. A brief look back

Already in 2008, Switzerland and the USA had concluded a framework with the same objective, the US-Swiss Safe Harbor Agreement. In its Schrems decision of 2015, the European Court of Justice (CJEU) held that the Safe Harbor Agreement between the EU and the US – which served as a model for the US-Swiss Safe Harbor Agreement – did not provide sufficient protection of personal data transferred to the US, considering the extensive surveillance activities by US authorities without adequate protection of private rights. Shortly after the Schrems decision, the Swiss Federal Data Protection and Information Commissioner (FDPIC) held that the US-Swiss Safe Harbor Framework suffered from the same flaws as the European equivalent.

Registration, Re-registration and Withdrawal

US Companies who want to benefit from Swiss recognition of adequate data protection, can register with and self-certify to the Department of Commerce (DoC) by publicly committing to comply with the Framework's requirements. While registration is completely voluntary, companies wishing to do so must confirm that they have data protection regulations in line with the principles of the Privacy Shield, which thereby become enforceable against such companies under US law.

Currently, there are 3,106 certified companies under the Swiss US Privacy Shield Framework and 4,676 companies certified under the EU-US Privacy Shield.

While the number of registered organizations shows that the Privacy Shield Frameworks are not ignored, standard clauses in bilateral agreements and group wide binding policies continue to be widely used also in the Swiss-US context as alternative or as complementary safeguards.

Organizations participating in the Privacy Shield Framework are required to *re-certify* to the DoC annually and to pay renewal fees to the ADR organization and the ICDR (see below).

An organization is free to *withdraw* from the Privacy Shield Framework, but must continue to apply the Privacy Shield Principles to the personal data received while it participated in the Privacy Shield and annually affirm to the DoC its commitment to apply the principles of the Privacy Shield to these data. Its listing as inactive remains publicly accessible on the web-site of the Privacy Shield.

Requirements

The main requirements for a certified organization relate to information to the data subject, data integrity and purpose limitations, data retention, accountability for data transferred to third parties, and transparency related to enforcement actions (if the Privacy Shield participant becomes subject to an FTC or court order based on non-compliance). A participant must inform individuals of their rights to access their personal data, of the participant's duty to disclose personal information in response to lawful request by public authorities, and the participant's liability in cases of onward transfer of data to third parties.

The DoC does not actively check compliance with all principles and specifications of a company seeking certification or re-certification. Only the fulfilment of the following conditions are subject to a detailed examination:

- Registration with a provider of an Independent Recourse Mechanism (*IRM*) (see below)
- Payment of the fees to the ICDR
- Compliance with the principle of access
- Completeness and consistency of the information submitted
- Privacy notices

Recourse and Remedies

Data subjects may file complaints alleging a violation of the Privacy Shield principles, e.g., that a registered company does not process its personal data correctly in accordance with the principles of the Privacy Shield. Under the privacy shield framework, a private person may file a complaint directly with the registered organization, through the independent recourse mechanism or with the FDPIC.

1. Direct complaint with the registered organization

If a private person is of the opinion that a registered organization does not comply with the provisions of the Privacy Shield and violates its related obligations on the protection of per-

sonal data, the first and most obvious step is to contact that organization directly. The company is obliged to reply to each complaint that is not manifestly ill-founded within 45 days after receipt. The reply must state whether the complaint is justified and if so what kind of measures the company intends to take in order to rectify a past violation and/or to avoid future violations.

2. Complaint with an independent body

Certified companies are obliged to make an independent recourse mechanism (IRM) available. Complainants can choose whether they want to file a complaint through the IRM directly or after having filed a complaint with the registered organization, whereby the latter is encouraged. The registered organisation can choose whether to designate as dispute resolution body the FDPIC or a private IRM provider based either in Switzerland or in the US. Registered organizations receiving employee data for human resource purposes have to choose the FDPIC.

a) FDPIC

The FDPIC will send its decision ("advice") to the registered organization and the complainant as soon as possible, but no later than within 60 days of receipt of the complaint. The company has 25 days to comply or respond to the advice of the FDPIC. If the registered organisation does not comply, the FDPIC may refer the case to the Federal Trade Commission (FTC) to initiate enforcement actions. It may also inform the DoC of the refusal to comply and request the deletion of the organization from the Privacy Shield list.

b) Alternative Dispute Resolution (ADR)

If the registered organization opts for a private ADR mechanism, its website must make clear which ADR institution has been designated and contain a link to the respective website providing information about the ADR's services, the address where to send the complaint and the procedure to be followed. The IRM must be free of charge to the complainant.

If a registered organization designates the same undertaking as ADR body which had already implemented and monitored its compliance with the Privacy Shield principles, it must make sure to avoid any potential conflicts of interest that may arise from this double role.

The ADR organizations designated most often are the Council of Better Business Bureaus (BBB), JAMS, and TRUSTe.

c) FTC

There is also the possibility to lodge a complaint directly with the FTC.

d) Ombudsperson

President Trump nominated Keith Krach, former CEO of DocuSign, as the next Under Secretary of State for Economic Growth, Energy and the Environment ("the E"), who will also serve as the Privacy Shield Ombudsperson. He has received unanimous endorsement by the Senate Foreign Relations Committee, his confirmation by the Senate seems to be a formality.

In his function as Privacy Shield Ombudsperson, Mr Krach will hear requests relating to personal data transmitted from the EU to the US being accessed by US intelligence authorities for national security purposes. Such requests may rely not just on the Privacy Shield, but also on standard contractual clauses (SCCs), binding corporate rules (BCRs) or similar frameworks.

His independency from the public administration is questionable, given the nomination by the President, but the personal integrity of Mr. Krach has not been questioned.

3. Numbers

The number of complaints that have been filed and dealt with directly between the complainants and certified companies is unknown. The FDPIC in his yearly report lists ten cases of

legitimate complaints filed with independent ADR bodies and none with the FDPIC. JAMS reports two cases in 2018. Representatives of the DoC stated on Oct. 18, 2018, that the total number of complaints filed across all of the IRM providers was less than 40.

4. Arbitration

a) Requirements and procedure

As an ultima ratio a complaint can be filed with the competent body for binding arbitration. Procedures before the arbitral tribunal can be initiated only after all of the above mentioned remedies have failed. Arbitration is open only to an affected data subject (physical person), not to registered organization or a third party. Arbitration is available only to determine whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation has remained fully or partially unremedied. The individual cannot invoke arbitration if he or she alleges that the Privacy Shield Principles are inadequate, or that these principles were unjustly encroached upon by a state asserting national security or other public interests.

Before initiating arbitration, the complainant must formally notify the respective registered organization of his or her intention.

The arbitral tribunal consists of one or three arbitrators, picked from a list of 26 arbitrators. Five of the arbitrators on the list were specifically nominated for the Swiss US Privacy Shield, 21 for the EU US Privacy Shield.

A Privacy Shield Arbitration Panel has the authority to impose relief such as access, correction, deletion, or return of the individual's data in question. It cannot award damages, costs, fees, etc.

Each party bears its own attorney's fees in the arbitration.

Arbitral awards are binding and enforceable before US courts and in almost all other jurisdictions. The seat of the arbitration is in the USA. The International Centre for Dispute Resolution (ICDR) of the American Arbitration Association (AAA) manages the Privacy Shield arbitration, while the procedure is governed by specific Privacy Shield Arbitration rules, which are modeled after the AAA Arbitration rules.

Arbitration proceedings are not available if a complaint has already been the subject of arbitration or state court procedure, or if the complaint has been clarified otherwise.

In addition, the FTC can initiate investigations in parallel to the arbitration proceedings.

b) Is arbitration an appropriate remedy?

The arbitration foreseen in the Swiss/European US Privacy Shield Frameworks has been harshly criticized as ignoring consumer protection concerns. The efforts and costs for the individual complainants in connection with an arbitration procedure seem unreasonably high. Considering the high complexity of the disputes, individuals are forced to seek legal representation by specialized attorneys, whose costs the individual complainant has to bear even if he wins. It is expected that the only arbitration procedures that we will see will be those financed by specific interest groups.

About the author:

Dr. Reinhard Oertli, Attorney at Law, is Partner at Meyerlustenberger Lachenal, Zurich. He is a member of the Legal Committee of the Swiss-American Chamber of Commerce.