Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 Para. 1 Swiss Federal Act on Data Protection

1. Significance and impact of the Federal Data Protection and Information Commissioner (FDPIC) list of countries

In accordance with Art. 7 OFADP,[1] the FDPIC maintains a list of countries documenting the adequacy of data protection in these countries within the meaning of Art. 6 FADP.[2] This list is publicly available.

In maintaining the list, the FDPIC takes the following into consideration:

- Legislation and its practical application by the individual countries and how this legislation is assessed by academia and courts;
- Conventions, publications, official statements and decisions by domestic and foreign institutions and authorities on the equivalence or adequacy of the level of data protection afforded by other countries or international organisations.

As a result of a large number of country decisions on the adequacy of data protection, Switzerland, together with the countries of the European Union (EU), the European Economic Area (EEA), and some non-European countries such as Argentina, Canada, New Zealand and Uruguay, now belongs to a group of nations which mutually assume the existence of an equivalent and adequate level of data protection.[3] This means that, generally, personal data can be transferred between Switzerland and other countries in the group without any special safeguards within the meaning of Art. 6 Para. 2 FADP, as it is the case for data transfers in a domestic context.

When these countries assess the adequacy of another country's data protection levels, its data protection legislation is considered as a whole, including the requirements which apply when personal data exchanged between the countries concerned is exported to a third country. There is thus a shared expectation between these countries – i.e. also between Switzerland and the EU and EEA member states – that the list of countries will be kept updated in such a way that the level of protection considered mutually adequate will be respected at all times. A mutual need for coordination arises in particular when the adequacy of a third country has been reassessed, as it is currently the case in the EU/EEA member states[4] following the latest ruling by the Court of Justice of the European Union (CJEU) with regard to the USA.

---

[1] Ordinance of 14 June 1993 to the Federal Act on Data Protection, SR 235.11

[2] Federal Act of 19 June 1992 on Data Protection, SR 235.1

[3] *Cf.* in particular decisions by the European Commission in application of Art. 25 of the Directive and also Section 2.3.3 of the FOJ explanations on the revision of the Ordinance to the Federal Act of 14 June 1993 on Data Protection: explanations on the draft of 18 January 2007, which still refer to Directive 95/46/EC of 24 October 1995.

[4] The repeal of the adequacy finding is directly applicable in the EEA-EFTA countries.

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

The list serves as a tool for Swiss data exporters, providing a general assessment by the authorities of the level of data protection in the listed countries, but one that is refutable. The list does not free data exporters of their obligation to question the presumed level of protection if there are indications of data protection risks in a specific case nor, if necessary, to apply safeguards in accordance with Art. 6 Para. 2 FADP - or even to refrain from exporting data altogether.

The list and the associated assessments are conditional on possible deviations in rulings by the Swiss courts, which would need to be considered by the FDPIC.

2. Placement of the United States of America on the list

The first column on the FDPIC's list of countries features those countries whose legislation can be considered to provide adequate protection within the meaning of Art. 6 Para. 1 FADP. Since the list was first kept, the US has not featured in this column. Therefore, when personal data is transferred from Switzerland to the US, the safeguards listed in Art. 6 Para. 2 FADP have to be applied in general.

2.1 Simplified data transfer under the Privacy Shield

Following partial simplification of data transfer, since 11 January 2017 the FDPIC has placed the USA on the list of countries in the second column, entitled 'Adequate protection under certain circumstances'. In the 'Remarks' column, an adequate level of data protection within the meaning of Art. 6 Para. 1 FADP is partially assumed for the USA, with reference to the Privacy Shield regime, which is based on unilateral declarations between the US and Swiss governments of 9 and 12 January 2017 respectively (hereinafter PS CH). The assumption is partial because it is restricted to data transfers directly involving US businesses that have signed up to a specific certification procedure under Privacy Shield regimes agreed between the US and Switzerland on the one hand and the US and the EU on the other, separately yet according to practically identical rules.[5]

2.2 Annual assessment

The PS regime includes an annual joint review of its functioning. Since the PS CH was set up, two such joint reviews have been conducted by the Swiss delegation (SECO, FDPIC) and the US government authorities (on 20 October 2018 and 14 September 2019). In each case, the review was conducted following the joint reviews by representatives of the European Commission and of the European Data Protection Board (EDPB), which were attended by a Swiss delegation having observer status.

[5] *Cf.* also notifications by the FDPIC at:
https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

When the USA's position on the list was last updated on 11 January 2017, the FDPIC expressly reserved the right to undertake adjustments to the list should he consider this to be appropriate based on his understanding of how the US actually implements the PS CH and in the light of decisions by the Swiss courts and possibly also the judiciary in the EU.[6]

2.3 US authorities' access to personal data

The PS regime with Switzerland provides solutions in two areas of application: data exchange in a commercial context, i.e. certified US businesses respect the principles of Swiss data protection legislation; and guarantees provided by the US authorities in relation to access to transferred personal data. The latter pertains in particular to the mass collection of non-US citizens' data for the purposes of anti-terrorism measures and national security.[7] Such access takes precedence over agreements for commercial purposes between Swiss and US contracting parties.

The FDPIC has based its assessment of access by the US authorities primarily on the information given in the EU reviews mentioned above. Therefore and in view of the fact that Switzerland and the EU mutually recognise their data protection legislation as equivalent, the FDPIC agrees with most of the EDPB's criticisms regarding access by US authorities, insofar as these can also be derived from Swiss data protection law.

For example, the FDPIC noted in his review reports that persons concerned in Switzerland do not have sufficient enforceable legal rights in the US, especially since the effectiveness of the ombudsperson mechanism, which is intended to guarantee an indirectly enforceable legal remedy, cannot be assessed owing to lack of transparency. Furthermore, the FDPIC criticised the fact that, without sufficiently concrete and conclusive information, it is not clear that the ombudsperson has decision-making powers vis-à-vis the US intelligence services nor enjoys actual independence. Safeguards are therefore lacking, a situation which, in view of the right to legal recourse afforded by Art. 29 et. seq. of the Federal Constitution of the Swiss Confederation (FC),[8] is highly problematic for the enforcement of the rights of persons concerned in Switzerland in accordance with Art. 13 Para. 2 FC and Art. 8 ECHR[9].[10] Despite these objections, the FDPIC left the entry regarding the level of data protection in the US

---

[6] *Cf.* FDPIC announcement of 11 January 2017: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows/transfer-of-data-to-the-usa/swiss-us-privacy-shield--new-framework-for-the-transfer-of-data-.html

[7] In accordance with Section 702 Foreign Intelligence Surveillance Act (FISA) and Executive Order 12 333 (EO 12 333).

[8] Federal Constitution of the Swiss Confederation, SR 101

[9] European Convention on Human Rights, SR 0.101

[10] *Cf.* https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html. In order for individuals to be able to effectively assert data protection rights arising from Art. 13 Para. 2 FC, they must be able to enforce their rights by legal means if necessary. The fundamental right to protection against data misuse therefore also includes a right to **legal protection** (Eva Maria Belser, at Belser/Epiney/Waldmann, Datenschutzrecht, § 6 N 104).

unchanged on his list of countries. Initially, like the EDPB, he wanted to allow the US to undertake improvements. Furthermore, by doing so no threat was posed to the application of the PS regime for the Swiss parties of certified US companies.

2.4 CJEU ruling on Schrems II

Unfortunately, the US has not yet introduced improvements in this regard, despite the criticism expressed by the EU and Switzerland in the PS evaluations and the discussions on this issue in the US Congress.[11] This is the context in which the ruling of 16 July 2020 by the CJEU)in the case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (hereinafter CJEU ruling)[12] declared the Adequacy Decision 2016/1250 by the EU Commission regarding US companies certified under the PS regime invalid.[13]

Thus, in consideration of the CJEU ruling, all exports of personal data from the EU to the US are henceforth subject to the requirements of Art. 46 of the EU General Data Protection Regulation (GDPR). According to the ruling, data processors are the primary instance responsible for assessing on a case-by-case basis whether the standard contractual clauses (SCCs)[14] in accordance with Art. 46 Para. 2 GDPR allow data to be exported to the US in a manner compatible with EU law; secondary responsibility lies with the data protection authorities in the EU member states. If data cannot be transferred in a compatible manner, data exports from the EU to the US should be stopped by the responsible parties either on their own initiative or at the behest of the data protection supervisory authority of the competent EU/EEA member state, and any personal data already exported should be deleted (for EEA, *cf.* footnote 4).

In view of the fact that SCCs cannot legally prevent foreign security services from accessing data, the CJEU referred to the EDPB, which is now responsible under Art. 65 Para. 1 c GDPR for establishing the necessary rules for the protection of data of the EU/EEA residents concerned (for EEA *cf.* footnote 4). To date, the EDPB has published FAQs dated 23 July 2020,[15] which will be amended on an ongoing basis.

---

[11] FISA 702 was extended in 2018 for a further six years (FN1 - PUBLIC LAW 115–118—JAN. 19, 2018). There has now also been public criticism of FISA in the US, but this has not led to any tangible improvements in data protection for inhabitants of Switzerland. Nor is this circumstance affected by the currently pending draft laws relating to FISA.

[12] http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18

[13] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016D1250

[14] Standard Contract Clauses

[15] https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en

3. Update re position of USA on list

3.1 Significance of the CJEU ruling for the Swiss economy

As Switzerland is not a member of the EU, it is not legally bound by the CJEU ruling.

Pursuant to Art. 3 GDPR, however, EU data protection law and any CJEU rulings based thereon shall be applied by authorities and courts in the EU and EEA with respect to Swiss companies if the latter process data in the way cited therein. Swiss companies must therefore assume that these foreign authorities may require them to observe EU law when exporting personal data, and may incur a fine if they fail to do so, in particular when processing the data of EU and EEA data subjects (with regard to the EEA, *cf.* footnote 4).

There is currently no legal decision in Switzerland comparable to the CJEU ruling. It is therefore unclear whether Swiss courts, in applying Art. 6 of the Swiss FADP, would reach similar conclusions regarding the access to data by US authorities as the CJEU has in applying the GDPR.

In view of this situation, the FDPIC, in consideration of the general principle of the rule of law and the need for legal certainty, feels compelled not only to reassess the current position of the US on the list, but also to provide more detailed legal justification for any amendment to it.

3.2 Principles of lawful data processing according to FADP is violated

The FDPIC stated in the review reports mentioned above that:

- for persons concerned in Switzerland there is no enforceable legal remedy with regard to the data access by US authorities, especially since the effectiveness of the ombudsperson mechanism, which is intended to guarantee an indirectly enforceable legal remedy, cannot be assessed due to a lack of transparency;
- that the decision-making powers of the ombudsperson vis-à-vis the US intelligence services and its actual independence cannot be assessed owing to a lack of clear and conclusive information.

The FDPIC considers that this lack of transparency and the resulting absence of guarantees concerning the interference of US authorities with privacy and informational self-determination of persons concerned in Switzerland is irreconcilable with:

- the right of such persons to legal recourse in accordance with Art. 29 ff. FC and Art. 15 FADP in order to assert the rights accorded to them by Art. 13 Para. 2 FC and Art. 8 ECHR[16]; and
- the principles of the lawful processing of personal data within the meaning of Art. 4 FADP.

[16] European Convention on Human Rights

3.3 Amendment of the countries' list

Because there is no guarantee of rights that would afford persons concerned in Switzerland protection comparable to that afforded by Art. 13 paras 2 and 29 ff. FC, Art. 8 ECHR and Art. 4 FADP, the FDPIC considers that data protection within the meaning of Art. 6 Para. 1 FADP is insufficient in the US, even for the processing of personal data by US companies that are certified under the PS regime. As a result of this assessment based on Swiss law, the FDPIC concluded that **the indication 'Adequate level of protection under certain circumstances' had to be removed for the US in the FDPIC's list of countries.**

As previously mentioned, this assessment by the FDPIC is subject to any deviating rulings by Swiss courts.

The FDPIC does not have such authority that his updated assessment, whereby the processing of personal data based on the PS CH fails to meet partial adequacy of data protection within the meaning of Art. 6 Para. 1 FADP, can influence the continuing existence of the PS CH regime. The regime can be invoked by persons concerned in Switzerland as long as it is not revoked by the USA. **The remarks on the PS regime in the country list will therefore remain, but has been adapted as follows:**

"Data processors who are on the list of the US Department of Commerce and sign up to the Privacy Shield regime between the US and Switzerland in relation to personal data obtained in Switzerland shall grant ***special protection rights*** *to persons in Switzerland****. However, these rights do not meet the requirements of adequate data protection as defined by the FADP****."*

4. Contractual Safeguards

Contractual safeguards such as the EU's SCCs, which are also frequently used in Switzerland, or so-called 'binding corporate rules' cannot prevent foreign authorities from accessing personal data if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency and legal protection of the persons concerned.[17] This is true not only in the case of transfer of personal data to the USA, but also to numerous other countries with inadequate legal protection, referred to here as 'non-listed countries'. Accordingly, it is to be assumed that in many cases the SCCs and comparable provisions do not meet the requirements for contractual safeguards pursuant to Art. 6 Para. 2 Let. a FADP for data transfer to non-listed countries.

[17] The same is true of the FDPIC's standard outsourcing agreement.

4.1 Practical advice for Swiss companies

When transferring data to non-listed countries in the future, data exporters should always consider each individual case with due diligence:

a) If the disclosure of data is based on contractual guarantees such as SCCs within the meaning of Art. 6 Para. 2 Let. a FADP, a risk assessment should be carried out. The exporter should check whether the clauses cover the data protection risks existing in the non-listed country. If necessary, the clauses should be expanded, although this in itself remains of limited effect if the public law of the given country takes precedence and deviates from these, as explained under b) below.

b) When examining data protection risks, it is of particular relevance whether the data is transferred to a company in a non-listed country that is subject to special access by the local authorities.[18] It must also be considered whether the foreign recipient company is entitled and in a position to provide the cooperation necessary for the enforcement of Swiss data protection principles. If this is not the case, any provisions in the SCCs concerning the obligation to cooperate are negated.

c) In such cases, the Swiss data exporter must consider technical measures that effectively prevent the authorities in the destination country from accessing the transferred personal data. If data is stored solely in the cloud by service providers in a non-listed country, for example, encryption would be conceivable, along the principles of BYOK (bring your own key) and BYOE (bring your own encryption), so that no individual personal data would be available in the destination country and if the service provider would have no possibility of decoding the data themselves. For services in the target country that go beyond mere data storage, however, the use of such technical measures is demanding. If such measures are not possible, the FDPIC recommends refraining from transferring personal data to the non-listed country on the basis of contractual guarantees.

4.2 Further information and advice

The FDPIC endeavours to provide Swiss companies with further information on the data-protection-compatible export of personal data to the US and other non-listed third countries in due course. He will do so as soon as further information such as relevant decisions by Swiss courts or statements from the EDPB are available.

[18] In the case of the US, exporters should ascertain whether the US companies in question fall under US laws on mass surveillance (esp. Section 702 FISA and EO 12 333), such as Electronic Communication Service Providers.