

Guide to checking the admissibility of direct or indirect data transfers to foreign countries (Art. 6 para. 2 letter a FADP)

(Published June 2021)

1 Purpose of the guide

This guide is intended to make it easier for data owners to check the permissibility of transfers of personal data abroad.

Based on a flow chart, this guide explains how Article 6 paragraph 2 letter a FADP applies if the foreign country concerned does not have legislation that ensures adequate protection and sufficient safeguards (see also Art. 6 para. 2 and 3 of the Ordinance to the Federal Act on Data Protection DPO, SR. 235.11). The requirements under letters b - g are not addressed in this guide.

SR 235.1 Federal Act on Data Protection (FADP)

Art. 6 Cross-border disclosure

- ¹ Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.
- ² In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:
- a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;

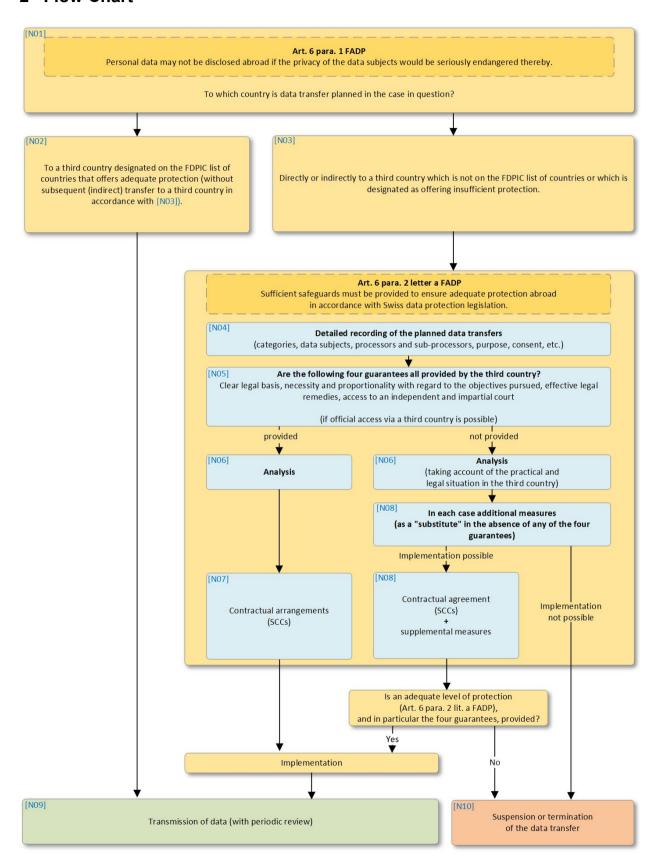
SR 235.11 Ordinance to the Federal Act on Data Protection (DPO)

Art. 6 Duty to provide information

- ² If the Commissioner has been informed of the safeguards and the data protection rules, the duty to provide information for all additional disclosures is regarded as fulfilled if such disclosures:
- a. are made subject to the same safeguards, provided the categories of recipient, the purpose the processing and the data categories remain essentially unchanged; or
- b. take place within the same legal person or company or between legal persons or companies that are under the same management, provided the data protection rules continue to ensure an adequate level of protection.
- ³ The duty to provide information is also regarded as fulfilled if data is transmitted on the basis of model contracts or standard contract clauses that have been drawn up or approved by the Commissioner, and the Commissioner has been informed about the use of these model contracts or standard contract clauses by the controller of the data file. The Commissioner shall publish a list of the model contracts and standard contract clauses that he has drawn up or approved.



2 Flow Chart





3 Explanatory Notes

[N01] Verification of the level of data protection in the third country

The data exporter must ensure that an adequate level of data protection is guaranteed when if the data is processed in the destination countries (Art. 6 FADP). If the data is transferred to an EU/EEA country, an adequate level of data protection can be assumed provided onward export to a third country is excluded.

It should be noted that a person contracted to process data in a country with an adequate level of data protection may, under certain circumstances, be subject to a law or other mandatory requirements of a third country which requires that person to disclose the data to the authorities of a third country; these disclosures may be non-transparent or non-justiciable (see in detail the guarantees in N05). In this case, proceed according to N03 (e.g., server in Switzerland, the EU or the EEA of a company that is directly or indirectly subject to the legal system of a country that does not have an adequate level of data protection).

[N02] Adequate Protection (art. 6 para. 1 FADP)

Exporting country figures on the FDPIC list of countries

If the owner of data collection transfers data to a country that is on the FDPIC's list of countries that have an adequate level of data protection, he is deemed to be acting in good faith pursuant to Article 3 para. 1 of the Swiss Civil Code ("CC"). However, this is a rebuttable presumption. The owner of the data collection cannot then invoke his good faith if he knows, for example, that in his specific case the adequate level of data protection is nevertheless not guaranteed in a particular country (Art. 3 para. 2 CC).

In any case, the data exporter remains responsible for the data export and must check periodically whether the protection is still adequate and if there are any other reasons (e.g., based on practical experience or reports in the media) to believe that personal data cannot be processed securely in the respective destination country.

Exporting country is not on the FDPIC list of countries

If a country is not on the FDPIC's list of countries, this does not automatically mean that it does not provide adequate protection. The FDPIC has not checked every country for adequacy. In addition, only a Swiss court can make a final binding decision on the application of Article 6 FADP. In this case, the data exporter must therefore carry out the necessary legal clarifications itself, *e.g.* by consulting literature and case law or obtaining independent legal advice.



[N03] No adequate protection according to the FDPIC list of countries or indication that no data transfer in conformity with data protection is possible (Art. 6 para. 2 letter a FADP)

If the country is not on the FDPIC's list of countries that offer adequate data protection or if, despite its presence on the list of countries, there are indications that an adequate level of data protection cannot be assumed for the intended export, the data exporter must ensure data protection by introducing sufficient safeguards, in particular by means of a contract. As a rule, **Standard Contractual Clauses (SCCs)** will be used as a basis. It should be noted that internal company data protection regulations, so-called **Binding Corporate Rules (BCR)**, which regulate the cross-border transfer of data within a group of companies or between different companies under uniform management, cannot be used by a data exporter in an external relationship as a substitute for SCCs. Individual BCRs can usually be amended by the data importer without the consent of the external data exporter and irrespective of the term of the contract, and they also lack essential components that are reflected in an SCC (e.g., provisions regarding the use of subcontractors).

[N04] Detailed records of the data transfer

The data exporter must keep detailed records of the data transfer, e.g., by means of a directory; these records form the basis for assessing the intended data export.

Among other things, the following must be clarified:

- Does the data to be exported relate to people?
- Are persons identified or identifiable?
- What is the purpose of the data disclosure?
- What categories of personal data are being transferred?
- Are there other contractors and subcontractors and are they located in third countries?
- Is the personal data going to be processed by companies that are subject to legal systems in third countries (e.g., US cloud providers with servers in CH/EU/EEA).
- Is the data going to be transferred within the third country or to another third country, or are there indications that this could happen?

[N05] Four Guarantees

With regard to official access in the third country (e.g. for national security or criminal investigation purposes) and the rights of the data subjects, the data exporter must check whether such access and rights are compatible with Swiss data protection law and Swiss constitutional principles. He must carry out the relevant evaluations himself and may not rely solely on the statements of the data importer. He can do this by consulting literature and case law or obtaining independent legal advice.



Rights equivalent to the following Swiss fundamental rights must be guaranteed in the third country, and it must be examined which deficiencies exist in the third country:

1. Principle of legality: clear, precise and accessible rules (art. 5 and art. 164 Federal Constitution "FC").

Sufficiently specific and clear legal provisions on the powers of public authorities and the purposes of, and procedures and substantive requirements for access to data by public authorities.

2. Proportionality of the powers and measures regarding the regulatory objectives pursued (Art. 5 para. 2 FC and Art. 4 para. 2 FADP)

The powers and measures available to the authorities must be suitable and necessary for the authorities to fulfil the legal purposes of their access. In addition, they must be reasonable as far as the data subjects are concerned.

3. Effective legal remedies must be available to the individual (Art. 13 para. 2 FC for the enforcement of Art. 15 FADP and Art. 8 ECHR)

Data subjects in Switzerland must have an effective legal remedy enshrined in law to enforce their rights to privacy and information-related self-determination (e.g. rights of access, rectification and deletion).

4. Guarantee of legal recourse and access to an independent and impartial court (Art. 29 ff. FC and art. 15 FADP).

Intrusions on privacy and information-related self-determination must be subject to an effective, independent and impartial monitoring system (court or other independent body, e.g. administrative authority or parliamentary body). In addition to prior (judicial) approval of surveillance measures (protection against arbitrary action), it must also be possible to verify the actual functioning of the surveillance system.

Note on the USA

If there are indications that personal data is or could be processed directly or indirectly in the USA when using cloud services, the questionnaire in the appendix can be used for further clarification ["Data protection inquiry to service providers/providers with possible direct or indirect US relationships (including their subcontractors and further sub-contractors and other service providers/providers)"].

[N06] Analysis

An analysis of the data transfer must be carried out in the individual case and in relation to the selected instrument, such as SCCs, and of the legal circumstances in the third country. The data exporter must make all the necessary inquiries when gathering and analysing the data transfer (e.g. obtaining independent legal opinions).



The following, among others, must be included in the examination:

- Applicable legislation in the country of destination
- Practices of the administrative and judicial authorities
- Case law

[N07] Guarantees given: SCC

If the four guarantees (see N05) are given, an adequate level of data protection can be achieved with standard SCCs.

All that then remains to be considered in the individual implementation of the SCCs is whether further contractual measures for individual protection (i.e. not against state access) are necessary. Such measures may include the following, for example:

- Enhanced rights for data subjects (e.g. right to information)
- Data transfers made conditional on technical measures being in place
- Enhanced powers for data exporters by requiring data importers to allow inspections of and be held accountable for data processing systems
- Clauses that enable and provide for rapid data backup procedures when needed.

[N08] Guarantees not given: SCCs and Mandatory Supplemental Measures

If the guarantees mentioned in N05 are not comprehensively given in the third country, additional measures that serve as "substitutes" for the missing four guarantees must be examined in advance in each case.

Additional contractual measures (between the data exporter and the data importer) are rarely possible because they cannot bind third-country authorities and thus cannot prevent unauthorised access. For example, compensation arrangements, assurances that legal action will be taken and legal remedies exhausted in response to official orders, or transparency reports are also insufficient, especially if legal requirements in the third country take precedence over or thwart contractual measures.

The additional technical and organisational measures must be such that the authorities in the destination country are effectively denied access to the personal data. In the case of data storage in the form of a simple cloud operation by service providers in a country without an appropriate level of protection, encryption would be conceivable, for example, if it is implemented according to the principles of both BYOK ("bring your own key") and additionally BYOE ("bring your own encryption"), so that no clear data is available in the cloud or no decryption and encryption takes place in the cloud. In the case of services in the target country that go beyond simple data storage, however, the use of such technical measures is challenging.

If the check shows that the lack of one or more of the four guarantees in N05 cannot be compensated for by additional measures, the procedure in N10 must be followed.



[N09] Data Transmission

After implementing the necessary additional measures, the data exporter must regularly review the technical and legal requirements. If he concludes that there is no longer any data protection compliance, he must proceed in accordance with N10.

[N10] Suspension or Termination of Data Disclosure Abroad

If additional measures cannot compensate for the identified deficiencies in fulfilling the four guarantees and that there is therefore no sufficient guarantee pursuant to Article 6 para. 2 letter a FADP, the data transfer abroad must be suspended or terminated immediately.



Annex¹

Data protection inquiry to service providers/suppliers with possible direct or indirect US relationships (including their subcontractors and further sub-subcontractors and other service providers/suppliers)

Service providers/supplier including all subsequent subcontractors and service providers/suppliers involved (including those for software components), referred to below as "vou"

In view of the judgment of the Court of Justice of the European Union in Case C-311/18, and in particular but not exhaustively paragraphs 138 to 145 thereof, we request the clarification of the following questions as a matter of urgency:

1	Direct Application of 50 U.S.C. § 1881a (= FISA 702)										
1.1 Do you or any other relevant US entity (controller or processor) that processes of to personal data that is transferred to you fall under any of the following def U.S.C.§ 1881(b)(4) that could render you or the other entity(ies) directly subject § 1881a (= FISA 702)?											
	□Y	'es	□ No	\square We are under a legal obligation not to answer this question							
1.2 Especially,											
A. are you or any other relevant US entity a telecommunications carrier, as that fined in section 153 of title 47 U.S.C.?											
		□ Yes	□ No	\square We are under a legal obligation not to answer this question							
		•	-	other relevant US entity a provider of electronic communication services, defined in section 2510 of title 18 U.S.C.?							
		□ Yes	□ No	☐ We are under a legal obligation not to answer this question							
		C. are you or any other relevant US entity a provider of a remote computing service, as that term is defined in section 2711 of title 18 U.S.C.?									
		□ Yes	□ No	☐ We are under a legal obligation not to answer this question							
	ŀ	are you or any other relevant US entity any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored?									
		⊒ Yes	□ No	☐ We are under a legal obligation not to answer this question							

¹ The present questionnaire was adapted to Swiss law requirements and further developed based on the questionnaire from www.noyb.eu.



E. are you or any other relevant US entity an officer, employee, or agent of an entity scribed in (A), (B), (C), or (D)?											
☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question											
Indirect Enforcement of FISA 702											
2.1 Are you controlled by a US parent company or shareholder, or do you have another relev tie to the US that could make US law indirectly enforceable against you?											
\square Yes \square No \square We are under a legal obligation not to answer this question											
If so, are you, as a matter of EU law, national law, corporate or private international law, required to ignore any order, request or directive from a US entity that would require you to expose any of the personal data that you process to the U.S. government under 50 U.S.C. § 1881a (= FSIA 702) or EO 12.333 and are you in fact able to block such access?											
\square Yes \square No \square We are under a legal obligation not to answer this question											
Please specify what legal and/or technical protections you rely on:											



Processing under EO 12.333 Do you, or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you, cooperate in any respect with US authorities conducting surveillance of communications under EO 12.333, irrespective of whether such cooperation is mandatory or voluntary? ☐ Yes □ No ☐ We are under a legal obligation not to answer this question Other relevant Laws 5 Are you or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you subject to any other law that could be seen as undermining the protection of personal data under the GDPR (Article 44 GDPR) or under Swiss law? ☐ Yes □ No \square We are under a legal obligation not to answer this question If you have answered 'yes' to the previous question, please specify these laws:



7

6	Measures against Mass and Indiscriminate Processing in Transit (FISA 702 and						
	12.333)						

As the Court of Justice has also highlighted the need to ensure that personal data is not subject to mass surveillance in transit, we seek the following clarifications:

A.	GDPR) inate pro	or every	step of the	e process al data by	ing oper y or on b	ations whic	ch ensure th uthorities in	at mass a	ee Article 32 nd indiscrim- uch as under	
	□ Yes	□ No	□ We ar	e under a	legal ob	oligation no	ot to answer	this ques	tion	
B.	organisa nor meta	itional m adata ca	easures (i	ncluding essed by	encrypti sophist	on) have b	een taken s	so that ne	echnical and ither content ccess to the	
W	/e ask yοι	ı to answ	bove quester these of this quest	questions		undue dela	ay, but no la	ter than fi	ve working	
[Place	[Place and Date]						[Company]			
						[Legally b	inding signa	ature]		