

EU SCC Transfer Impact Assessment (TIA)

iapp If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

Author: David Rosenthal (original version at www.rosenthal.ch)
(Licensing: See bottom)

Version 1.01 (September 1st, 2021)

(Version for transfers to USA)

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The green text is mere sample text; the values and reasoning do not necessarily represent the author's opinion and are given for illustration purposes only.

Step 1: Describe the intended transfer			
a)	Data exporter ¹⁾ (or the sender in case of a relevant onward transfer):	ACME Europe GmbH, ACME France SAS, ACME Switzerland AG	
b)	Country of data exporter:	Germany, France and Switzerland	
c)	Data importer ²⁾ (or the recipient in case of a relevant onward transfer):	ACME Inc.	
d)	Country of data importer:	USA	
e)	Context and purpose of the transfer:	Compliance and Workforce Statistics by ACME Inc.	
f)	Categories of data subjects concerned:	Employees	
g)	Categories of personal data transferred:	HR data, including identifying information, job data, salary data, diversity information (where available)	
h)	Sensitive personal data:	data on race, sexual orientation	
i)	Technical implementation of the transfer:	Remote online access to HR system by parent company, with the ability to download data	
j)	Technical and organizational measures in place (optional):	IGDTA, individual access control on need-to-know-basis, encryption in-transit & at-rest, data loss prevention and endpoint protection systems, NDAs, instructions, trainings and audits (for more, see IGDTA)	
k)	Relevant onward transfer(s) of personal data (if any): ³⁾	Processing done by HostingCo Corp.	→ perform separate TIA
l)	Countries of recipients of relevant onward transfer(s):	USA	

Step 2: Define the TIA parameters			
Reasoning			
a)	Starting date of the transfer:	1-Sep-21	
b)	Assessment period in years:	5	Once we approach the end of the period, we will re-assess the situation.
	Ending date of the assessment based on the above:	1-Sep-26	
c)	Determining the acceptable residual risk of foreign lawful access: If the probability of a lawful access happening in the assessment period is so low that the chances of it are still only at 50:50 if another xx years were to pass by, then the probability of it happening in the initial period is so low that we have no reason to believe that it will occur in such period. What should xx be? ⁴⁾	30	(= in total 35 years)
	Probability permitted calculated based on the above (alternatively, you can manually override this value ⁵⁾):	9.43%	30
d)	Target jurisdiction for which the TIA is made:	USA	(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	Section 702 FISA, EO 12.333 (and PPD-28)	
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged? ⁶⁾	50%	This value is not relevant in our case. We have left it unchanged.

Step 3: Define the safeguards in place			
Reasoning			
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? ⁷⁾	No	The analysis needs to be done by the parent company, which is located in the US. This is also where the staff performing such analysis is located.
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No	n/a
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? ⁸⁾	No	Ensure that data remains encrypted All traffic over telecom lines is protected by state-of-the-art line encryption (VPN).
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign lawful access is at least technically possible The parent company needs access to the HR data in clear text in order to be able to process it. Encryption is not possible.
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	Ensure that the mechanism remains in place and is complied with We have in place an IGDTA based on the new EU SCC, and we have no reason to believe that the parent company will not comply with them, to the extent that US law permits so. Regular audits confirm the adequacy of the data security agreed therein.
Based on the answers given above, the transfer is:		permitted, subject to Step 4	You can delete this after use or if not used

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction ⁹⁾			
Country-specific! The following factors have been drafted for US law ; amend as necessary for other jurisdictions.			
a)	Assess the probability that during the assessment period, the following legal arguments will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above: ¹⁰⁾		
		Probability of	Reasoning
		Probability of possibility of a (successfully) request?	

Decision support using "Delphi" Number of participants: 3

First Round					Second Round					Average
P1	P2	P3	P4	P5	P1	P2	P3	P4	P5	to be used

Hide sample with "x"

	The data importer/recipient is no "Electronic Communications Service Provider" ¹¹⁾ with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	90%	10.00%	In the context of the transfer, the parent company does not provide any cloud, data storage or communications service. It is using the data for its own purposes.
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws ¹²⁾	0%	100.00%	The parent company does have possession and, at least, control of the data.
	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request ¹³⁾	60%	40.00%	The parent company is a US person, and the data at issue is communicated to the parent. The transfer is therefore considered communications to a US person which is not subject to the relevant laws.
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request ¹⁴⁾	0%	100.00%	Given that the personal data is actually transferred and stored in the US, we do not believe that the applicability of European data protection law will prevent the access by the government.
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case ¹⁵⁾	0%	100.00%	n/a
b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts? ¹⁶⁾	Yes	100.00%	This is a requirement under the EU SCC entered into with the parent company.
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience? ¹⁷⁾ †††	5%	5.00%	The processed data is HR data of a company. This is not the target of data gathering under Section 702 FISA or EO 12.333. This is confirmed both by a report of the Privacy and Civil Liberties Oversight Board (PCL08) (https://bit.ly/3ye07us), the NSA's comments (https://bit.ly/3dFalkh), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQ8). These sources contain no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, we believe that the probability that the parent company has or will receive a surveillance order with respect to our data during the period under consideration is very low.
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	100%	100.00%	The parent company does have access to the data, at least the one that is downloaded, and can, therefore, search it.
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		We are regularly monitoring the legal development in this area (and at least annually). Also, we have agreed with the data importer to regularly report on its experience with lawful access requests.
Probability that legal arguments fail to prevent foreign lawful access: †††			4.00%	during the assessment period
Overall probability of a lawful access prohibited under applicable data protection laws:			0.20%	
In view of the TIA parameters, the residual risk of prohibited lawful access is:			acceptable	
Number of years it takes for a lawful access to occur at least once with a 90 percent probability:			5,751	
Number of years it takes for a lawful access to occur at least once with a 50 percent probability:			1,731	
... assuming that the probability neither increases nor decreases over time (like tossing a coin)				
We have made the assessment in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics):		With the help of experienced outside counsel and legal research, as indicated		
Final Step: Conclusion				
In view of the above and the applicable data protection laws, the transfer is:		permitted		Reassess at the latest by: 1-Sep-26
(or if there are any changes in circumstances)				
This Transfer Impact Assessment has been made by:		Place, Date:		
Willy Beachum, Legal Counsel, ACME US Inc.; Angela Bennett, Data Protection Officer, ACME Europe Ltd.; Mitch McDeere, Bendini, Lambert & Locke (outside counsel); Alice Pleasance Liddell, Head of HR, ACME US Inc.		Signed:		
Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and Importer.		By:		

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks only for the purposes of European data protection law, where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where any foreign lawful access is an issue, for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at [www.rosenthal.ch \(https://bit.ly/2V9dj7V\)](https://bit.ly/2V9dj7V), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schiems I" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

More on the Delphi-Method: https://en.wikipedia.org/wiki/Delphi_method

How to use "Delphi":

1. Enter the number of participants in the relevant field.
2. Mark the yellow fields in column J with an x. This will hide the sample text/number.
3. Start with the first line.
4. Have each participant think of an appropriate value for the line.
5. Put the value of each participant into the columns K-O; don't discuss yet.
6. Once completed, discuss the values; you may remove the "x" in column J.
7. Have each participant again think of an appropriate value.
8. Enter them into the columns P-T. The average in column U is the value to use.
9. Proceed with the next line and redo steps 4-9.
10. Look at and discuss the end result only once you are finished.

<p>† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).</p>
<p>†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) <i>possibility</i> of it occurring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.</p>
<p>††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)</p>
<p>¹⁾ The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.</p>
<p>²⁾ The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.</p>
<p>³⁾ Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.</p>
<p>⁴⁾ We have seen that many people have difficulties in coming up with a percentage figure for a probability of an event at which they "have no reason to believe" that it will occur (which is the test under the EU SCC and the EDPB guidance for the residual risk of a prohibited foreign lawful access). We also found that people are more comfortable in assessing the probability of an event by expressing its probability of occurring in number of years ("an earthquake of this kind is to happen only once in 100 years on average"). We, therefore, use this concept to calculate the "permitted" residual risk in percent. Because we are not assessing earthquakes (which happen in any event) we have set the benchmark at a 50% chance of a lawful access occurring. You can also use another value, but we believe that if a lawful access has a 50:50 chance of occurring it in our view has become an unacceptable risk. If it, however, takes a long period of time (for example an additional 30 years after our assessment period) for the chances to raise to that level (at which a lawful access is still far from certain statistically), many will conclude that the risk of it happening in the first (for example) five years of our assessment period is rather theoretical. We then, based on a statistics formula,² calculate the acceptable percentage value for our assessment period (which is then used in Step 4, if necessary).</p>
<p>⁵⁾ You do not have to use our "50:50 chances"-method of determining the maximum percentage for assessing the probability of lawful access that results from Step 4. If you wish, you can manually enter the percentage figure you think is still acceptable (thus overwriting the formula in the cell). The grey number on the right hand of the percentage figure will tell you what this will mean in terms of years when using our method. If you do not manually overwrite the percentage, you can ignore the grey number.</p>
<p>⁶⁾ You will normally not need to care about this figure. It becomes necessary if the importer does not have a "defend you data" obligation, i.e. is not obliged to challenge lawful access requests in its own jurisdiction. In these cases, we use this figure to determine the probability of the authorities obeying the law even if their lawful access requests are not challenged by the importer (if the importer does challenge the lawful access request, a court or other authority will usually determine whether the legal prerequisites for the lawful access are met). A value of 50% means that in half of the cases the authorities may issue and try to enforce a lawful access request even if the requirements of law are not met. If that happens, the assessment in Step 4 becomes partially moot, because it is based on the assumption that a lawful access will be successful only if the prerequisites set forth by law are met. With this figure we take this uncertainty into account if the importer is expected not to make sure that lawful access requests are challenged.</p>
<p>⁷⁾ This question is, in principle, not necessary for assessing the transfer. We have nevertheless included it because many data protection authorities will want to know whether the exporter has considered alternatives to transferring personal data into a non-whitelisted country and why they are not pursued*. The response has no impact on the outcome of the assessment but is for mere documentary purposes.</p>
<p>⁸⁾ This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).</p>
<p>⁹⁾ In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered not fulfilling in particular requirement (3) and (4). Hence, it has to be verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.</p>
<p>¹⁰⁾ Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at https://bit.ly/3r5v07D), the FAQ for company of NOYB (including forms to be sent to US providers, available at https://bit.ly/2V9eez7), the Swiss Federal Data Protection and Information Commissioner's guidance (available at https://bit.ly/37b59tl), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHMy7 and a full paper from the same author at https://bit.ly/2V9eez7 with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/312oH2.</p>
<p>¹¹⁾ Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "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." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (https://bit.ly/3lgt15t).</p>
<p>¹²⁾ For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (https://bit.ly/3l2afC9). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) with a summary of the standards of US law as to what amounts to "control".</p>
<p>¹³⁾ According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (https://www.nsa.gov/about/faqs/signif-faqs/#sigint4). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHMy7 and a full paper from the same author at https://bit.ly/2V9eez7 with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/312oH2.</p>
<p>¹⁴⁾ The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://bit.ly/3eV2tSq).</p>
<p>¹⁵⁾ An example could be the following case: The importer uses a piece of software for managing the data, which is technically not able to comply with a lawful access request (e.g., a CRM or ERP software with a proprietary database structure), but could be amended to do so. However, in the specific case, doing so would violate copyright law because the importer has no right to change the software or not the necessary information to do so. If this circumstance is not considered above in connection with having "control" over the data at issue or below as a technical barrier, it can be considered here as another (legal) obstacle towards compliance with the lawful access request.</p>
<p>¹⁶⁾ The legal arguments above are useless if it is not ensured that they are complied with in case of a specific lawful access request. This can be ensured by the importer challenging such requests (which, in turn, can be secured by having a corresponding "defend your data" clause in the contract, which the EU SCC have). If there is no such obligation to challenge such requests, the exporter will depend on the probability of the authorities at issue to comply with their own law, which is usually below 100%. The relevant percentage is taken from Step 2 and applied to the overall calculation.</p>
<p>¹⁷⁾ Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the <i>categories</i> of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLBO) (https://bit.ly/3y07u5s), the NSIC comments (https://bit.ly/3dFalkh), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3he8rQB). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).</p>
<p>* This form and the underlying method was developed by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP), Baltasar Cevc (Finglex), Katharina Koerner, David Vassella (WalderWyss), Josh Edgerly (IAPP) and others. David Rosenthal can be reached at david@rosenthal.ch (private) or rosenthal@vischer.com (office).</p>

DISCLAIMER: You are using of this spreadsheet and transfer impact assessment method on an "as is" basis without any implied or express warranties, and entirely at your own risk, as it may contain errors. It provided you for informational and research purposes only and does not replace getting professional legal advice. Please report me any errors you find or other thoughts you have, so that I can update the file. See also my original work on the topic (incl. a scientific paper in German), which is available at <http://www.rosenthal.ch> and the Excel specifically at https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

All rights in this spreadsheet and transfer impact assessment method are reserved. This file is made available under a free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license (<https://creativecommons.org/licenses/by-sa/4.0/>). The input fields (blue background) and sample text therein are not subject to the license and may be changed and shared. Attribution must also include reference to the link where the original and master version of this file can be obtained at www.rosenthal.ch. If you need a different license, contact me at david@rosenthal.ch.



EU SCC Transfer Impact Assessment (TIA)



If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

Author: David Rosenthal (original version at www.rosenthal.ch)*
(Licensing: See bottom)

Version 1.01 (September 1st, 2021)

(Version for transfers to USA)

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The **green text** is mere sample text; the values and reasoning do *not* necessarily represent the author's opinion and are given for illustration purposes only.

Step 1: Describe the intended transfer

a)	Data exporter ¹⁾ (or the sender in case of a relevant onward transfer):	ACME Inc.	
b)	Country of data exporter:	USA	
c)	Data importer ²⁾ (or the recipient in case of a relevant onward transfer):	HostingCo Corp.	
d)	Country of data importer:	USA	
e)	Context and purpose of the transfer:	Hosting of downloaded HR data	
f)	Categories of data subjects concerned:	Employees	
g)	Categories of personal data transferred:	HR data, including identifying information, job data, salary data, diversity information (where available)	
h)	Sensitive personal data:	data on race, sexual orientation	
i)	Technical implementation of the transfer:	HostingCo operates the servers on which ACME Inc. is storing the HR data it has downloaded	
j)	Technical and organizational measures in place (optional):	IGDTA, individual access control on need-to-know-basis, encryption in-transit & at-rest, data loss prevention and endpoint protection systems, NDAs, instructions, trainings and audits (for more, see IGDTA)	
k)	Relevant onward transfer(s) of personal data (if any): ³⁾	None	→ perform separate TIA
l)	Countries of recipients of relevant onward transfer(s):	n/a	

Step 2: Define the TIA parameters

Reasoning				
a)	Starting date of the transfer:	1-Sep-21		
b)	Assessment period in years:	5		Once we approach the end of the period, we will re-assess the situation.
	Ending date of the assessment based on the above:	1-Sep-26		
c)	Determining the acceptable residual risk of foreign lawful access: If the probability of a lawful access happening in the assessment period is so low that the chances of it are still only at 50:50 if another xx years were to pass by, then the probability of it happening in the initial period is so low that we have no reason to believe that it will occur in such period. What should xx be? ⁴⁾	30	(= in total 35 years)	We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.
	Probability permitted calculated based on the above (alternatively, you can manually override this value ⁵⁾):	9.43%	30	
d)	Target jurisdiction for which the TIA is made:	USA		(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	Section 702 FISA, EO 12.333 (and PPD-28)		
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged? ⁶⁾	50%		This value is not relevant in our case. We have left it unchanged.

Step 3: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? ⁷⁾	No		The analysis needs to be done by the ACME Inc., which is located in the US, and its provider needs to be located in the US for technical reasons.
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		n/a
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? ⁸⁾	No	Ensure that data remains encrypted	All traffic over telecom lines is protected by state-of-the-art line encryption (VPN).
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign lawful access is at least technically possible	The ACME Inc. needs access to the HR data in clear text in order to be able to process it. Encryption is not possible.
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	Ensure that the mechanism remains in place and is complied with	ACME Inc. has in place a contract with the provider that provides the same level of protection as do the EU SCC and are, thus, compliant with Clause 8.7 of the EU SCC, and we have no reason to believe that the provider will not comply with them, to the extent that US law permits so. Regular audits confirm the adequacy of the data security agreed therein.
Based on the answers given above, the transfer is:		permitted, subject to Step 4		

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction⁹⁾

Country-specific! The following factors have been drafted for **US law**; amend as necessary for other jurisdictions.

a)	Assess the probability that during the assessment period, the following <i>legal arguments</i> will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above: ¹⁰⁾			
		Probability†	Probability of possibility of a (successful) request‡‡‡	Reasoning
	The data importer/recipient is no "Electronic Communications Service Provider" ¹¹⁾ with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	0%	100.00%	The provider is clearly a ECSP.
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws ¹²⁾	0%	100.00%	The provider holds ACME Inc's data on its servers.
	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request ¹³⁾	75%	25.00%	ACME Inc. Is a US person and located in the US. Its data is stored in a dedicated area on the provider's servers separated from other customers, and is clearly known to be data of a domestic client. If the provider were ordered to search this data, it would be obvious that such search would intentionally target a US person. Hence, we believe that the relevant laws do not apply. A remaining uncertainty applies if the authorities were to argue that the data is, in reality, data of non-US-persons despite the foregoing.
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request ¹⁴⁾	0%	100.00%	Given that the personal data is actually transferred and stored in the US, we do not believe that the applicability of European data protection law will prevent the access by the government.
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case ¹⁵⁾	0%	100.00%	n/a

b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts? ¹⁶⁾	Yes	100.00%	This is a requirement under the EU SCC entered into with the parent company.
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience? ¹⁷⁾ †††	5%	5.00%	The processed data is HR data of a company. This is not the target of data gathering under Section 702 FISA or EO 12.333. This is confirmed both by a report of the Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit.ly/3yeO7us), the NSA's comments (https://bit.ly/3dFalkh), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQB). These sources contain no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, we believe that the probability that the provider has or will receive a surveillance order with respect to our data during the period under consideration is very low.
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	100%	100.00%	The provider does have access to the data, and can, therefore, search it.
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		We are regularly monitoring the legal development in this area (and at least annually). Also, we have agreed with the data importer to regularly report on its experience with lawful access requests.
Probability that legal arguments fail to prevent foreign lawful access: †††			25.00%	} during the assessment period
Overall probability of a lawful access prohibited under applicable data protection laws:			1.25%	
In view of the TIA parameters, the residual risk of prohibited lawful access is:		acceptable		
Number of years it takes for a lawful access to occur at least once with a 90 percent probability:		915		
Number of years it takes for a lawful access to occur at least once with a 50 percent probability:		276		
... assuming that the probability neither increases nor decreases over time (like tossing a coin)				
We have made the assesement in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics):		With the help of experienced outside counsel and legal research, as indicated		
Final Step: Conclusion				
In view of the above and the applicable data protection laws, the transfer is:		permitted	Reassess at the latest by:	1-Sep-26
(or if there are any changes in circumstances)				
This Transfer Impact Assessment has been made by:		Place, Date:		
Willy Beachum, Legal Counsel, ACME US Inc.; Angela Bennett, Data Protection Officer, ACME Europe Ltd.; Mitch McDeere, Bendini, Lambert & Locke (outside counsel); Alice Pleasance Liddell, Head of HR, ACME US Inc.		Signed:		

Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.

By:

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks *only for the purposes of European data protection law*, where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where *any foreign lawful access is an issue*, for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at www.rosenthal.ch (<https://bit.ly/2V9dj7V>), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schrems II" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).

†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) *possibility* of it occurring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.

††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)

¹⁾ The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.

²⁾ The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.

³⁾ Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.

⁴⁾ We have seen that many people have difficulties in coming up with a percentage figure for a probability of an event at which they "have no reason to believe" that it will occur (which is the test under the EU SCC and the EDPB guidance for the residual risk of a prohibited foreign lawful access). We also found that people are more comfortable in assessing the probability of an event by expressing its probability of occurring in number of years ("an earthquake of this kind is to happen only once in 100 years on average"). We, therefore, use this concept to calculate the "permitted" residual risk in percent. Because we are not assessing earthquakes (which happen in any event) we have set the benchmark at a 50% chance of a lawful access occurring. You can also use another value, but we believe that if a lawful access has a 50:50 chance of occurring it in our view has become an unacceptable risk. If it, however, takes a long period of time (for example an additional 30 years after our assessment period) for the chances to raise to that level (at which a lawful access is still far from certain statistically), many will conclude that the risk of it happening in the first (for example) five years of our assessment period is rather theoretical. We then, based on a statistics formula, calculate the acceptable percentage value for our assessment period (which is then used in Step 4, if necessary).

⁵⁾ You do not have to use our "50:50 chances"-method of determining the maximum percentage for assessing the probability of lawful access that results from Step 4. If you wish, you can manually enter the percentage figure you think is still acceptable (thus overwriting the formula in the cell). The grey number on the right hand of the percentage figure will tell you what this will mean in terms of years when using our method. If you do not manually overwrite the percentage, you can ignore the grey number.

⁶⁾ You will normally not need to care about this figure. It becomes necessary if the importer does not have a "defend you data" obligation, i.e. is not obliged to challenge lawful access requests in its own jurisdiction. In these cases, we use this figure to determine the probability of the authorities obeying the law even if their lawful access requests are not challenged by the importer (if the importer does challenge the lawful access request, a court or other authority will usually determine whether the legal prerequisites for the lawful access are met). A value of 50% means that in half of the cases the authorities may issue and try to enforce a lawful access request even if the requirements of law are not met. If that happens, the assessment in Step 4 becomes partially moot, because it is based on the assumption that a lawful access will be successful only if the prerequisites set forth by law are met. With this figure we take this uncertainty into account if the importeur is expected not to make sure that lawful access requests are challenged.

⁷⁾ This question is, in principle, not necessary for assessing the transfer. We have nevertheless included it because many data protection authorities will want to know whether the exporter has considered alternatives to transferring personal data into a non-whitelisted country and why they are not pursued⁴. The response has no impact on the outcome of the assessment but is for mere documentary purposes.

⁸⁾ This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).

⁹⁾ In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered *not* fulfilling in particular requirement (3) and (4). Hence, it has to be verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.

¹⁰⁾ Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at <https://bit.ly/3r5v070>), the FAQ for company of NOYB (including forms to be sent to US providers, available at <https://bit.ly/2Vozeb7>), the Swiss Federal Data Protection and Information Commissioner's guidance (available at <https://bit.ly/37b5tHs>), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at <https://bit.ly/3qHNMy7> and a full paper from the same author at <https://bit.ly/2V9veez> with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at <https://bit.ly/3l12oHZ>.

¹¹⁾ Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "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." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (<https://bit.ly/3lgsTt5>).

¹²⁾ For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (<https://bit.ly/3i2xfC9>). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (<https://bit.ly/3rLQfbp>) with a summary of the standards of US law as to what amounts to "control".

¹³⁾ According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (<https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4>). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at <https://bit.ly/3qHNMy7> and a full paper from the same author at <https://bit.ly/2V9veez> with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at <https://bit.ly/3l12oHZ>.

¹⁴⁾ The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (<https://bit.ly/3eVzLSq>).

¹⁵⁾ An example could be the following case: The importer uses a piece of software for managing the data, which is technically not able to comply with a lawful access request (e.g., a CRM or ERP software with a proprietary database structure), but could be amended to do so. However, in the specific case, doing so would violate copyright law because the importer has no right to change the software or not the necessary information to do so. If this circumstance is not considered above in connection with having "control" over the data at issue or below as a technical barrier, it can be considered here as another (legal) obstacle towards compliance with the lawful access request.

¹⁶⁾ The legal arguments above are useless if it is not ensured that they are complied with in case of a specific lawful access request. This can be ensured by the importer challenging such requests (which, in turn, can be secured by having a corresponding "defend your data" clause in the contract, which the EU SCC have). If there is no such obligation to challenge such requests, the exporter will depend on the probability of the authorities at issue to comply with their own law, which is usually below 100%. The relevant percentage is taken from Step 2 and applied to the overall calculation.

¹⁷⁾ Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the *categories* of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLOB) (<https://bit.ly/3yeO7us>), the NSA's comments (<https://bit.ly/3dFalkh>), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: <https://bit.ly/3heBYQB>). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).

* This form and the underlying method was developed by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP), Baltasar Cevc (Fingolex), Katharina Koerner, David Vasella (WalderWyss), Josh Edgerly (IAPP) and others. David Rosenthal can be reached at david@rosenthal.ch (private) or drosenthal@vischer.com (office).

DISCLAIMER: You are using of this spreadsheet and transfer impact assessment method on an "as is" basis without any implied or express warranties, and entirely at your own risk, as it may contain errors. It provided you for informational purposes only and does not replace getting professional legal advice. Please report me any errors you find or other thoughts you have, so that I can update the file. See also my original work on the topic (incl. a scientific paper in German), which is available at <http://www.rosenthal.ch> and the Excel specifically at https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

All rights in this spreadsheet and transfer impact assessment method are reserved. This file is made available under a free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license (<https://creativecommons.org/licenses/by-sa/4.0/>). The input fields (blue background) and sample text therein are not subject to the license and may be changed and shared. Attribution must also include reference to the link where the original and master version of this file can be obtained at www.rosenthal.ch. If you need a different license, contact me at david@rosenthal.ch.



EU SCC Transfer Impact Assessment (TIA)



If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

Author: David Rosenthal (original version at www.rosenthal.ch)*
(Licensing: See bottom)

Version 1.01 (September 1st, 2021)

(Version for transfers to USA)

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The **green text** is mere sample text; the values and reasoning do *not* necessarily represent the author's opinion and are given for illustration purposes only.

Step 1: Describe the intended transfer

a)	Data exporter ¹⁾ (or the sender in case of a relevant onward transfer):	ACME Europe GmbH, ACME France SAS, ACME Switzerland AG	
b)	Country of data exporter:	Germany, France, Switzerland	
c)	Data importer ²⁾ (or the recipient in case of a relevant onward transfer):	OfficeCloud LLC	
d)	Country of data importer:	USA	
e)	Context and purpose of the transfer:	Cloud-based office applications, mail server, sharedrives (SaaS)	
f)	Categories of data subjects concerned:	Employees, customer contacts, supplier contacts, other	
g)	Categories of personal data transferred:	E-mails, office documents (for service usage data and user account data, a separate TIA is to be performed, because it is subject to a separate risk profile)	
h)	Sensitive personal data:	All special categories of data are in principle possible	
i)	Technical implementation of the transfer:	The European entity of OfficeCloud provides the service to us; it operates its data center in Ireland (where data is at-rest), but its parent company in the US may gain access in certain cases for support purposes	
j)	Technical and organizational measures in place (optional):	IGDTA, individual access control on need-to-know-basis, encryption in-transit & at-rest, data loss prevention and endpoint protection systems, NDAs, instructions, trainings and audits (for more, see IGDTA)	
k)	Relevant onward transfer(s) of personal data (if any): ³⁾	n/a	→ perform separate TIA
l)	Countries of recipients of relevant onward transfer(s):	n/a	

Step 2: Define the TIA parameters

Reasoning				
a)	Starting date of the transfer:	1-Sep-21		
b)	Assessment period in years:	5		Once we approach the end of the period, we will re-assess the situation.
	Ending date of the assessment based on the above:	1-Sep-26		
c)	Determining the acceptable residual risk of foreign lawful access: If the probability of a lawful access happening in the assessment period is so low that the chances of it are still only at 50:50 if another xx years were to pass by, then the probability of it happening in the initial period is so low that we have no reason to believe that it will occur in such period. What should xx be? ⁴⁾	30	(= in total 35 years)	We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.
	Probability permitted calculated based on the above (alternatively, you can manually override this value ⁵⁾):	9.43%	30	
d)	Target jurisdiction for which the TIA is made:	USA		(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	Section 702 FISA, EO 12.333 (and PPD-28)		
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged? ⁶⁾	50%		This value is not relevant in our case. We have left it unchanged.

Step 3: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? ⁷⁾	No		No, we already have chosen to have our data to be stored at-rest in the European facility of the provider; although our data will be processed mainly in Europe, it can in certain cases not be excluded that the provider's parent may access it.
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		n/a
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? ⁸⁾	No	Ensure that data remains encrypted	All traffic over telecom lines is protected by state-of-the-art line encryption (VPN).
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign lawful access is at least technically possible	The parent of the provider may in certain cases need access to our data in clear text to provide the service. Full encryption (hold-your-own-key) is not possible in such a SaaS context.
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	Ensure that the mechanism remains in place and is complied with	The provider has in place the EU SCC within its organization, including between the European subsidiary and the parent company in the US.
Based on the answers given above, the transfer is:		permitted, subject to Step 4		

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction⁹⁾

Country-specific! The following factors have been drafted for US law; amend as necessary for other jurisdictions.				
a)	Assess the probability that during the assessment period, the following <i>legal arguments</i> will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above: ¹⁰⁾			
		Probability†	Probability of possibility of a (successful) request††	Reasoning
	The data importer/recipient is no "Electronic Communications Service Provider" ¹¹⁾ with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	40%	60.00%	The parent company may qualify as a ECSP for its US customers, but in terms of the services provided to its European subsidiary, it is only providing support services, and will in our view not qualify as an ECSP with regard to such activities. Hence, it would in our view not be subject to the relevant laws with regard to the European data to which it has access. We understand that this argument may not be shared by others, which is why we rate it very conservatively to be on the safe side.
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws ¹²⁾	60%	40.00%	The parent company has no possession or custody of the customer data, as it is stored in the data centers of its European subsidiary. We also believe that it has no legal or day-to-day control over the customer data, as it is granted access only on a case-by-case-basis in selected support cases and only if the customer approves ("lockbox"). The data is encrypted with access permitted in principle only by the customer's own users, not the provider. Under its contract with its European subsidiary, too, the parent is legally not permitted to access unencrypted customer data without prior customer approval. We believe that this will allow for a reasonable argument that there is also no control.

	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request ¹³⁾	20%	80.00%	<i>If the data is transferred to the US, it is done so by its wholly- owned subsidiary because it needs the assistance of its parent company, and because the parent company (not the customer) has instructed it to get such assistance in such cases. Hence, such transfers of customer data are in essence intra-group communications initiated by, and controlled, by a US person in order to enable the subsidiary to fulfil its contract. Such kind of communications may not be targeted by the US government under the relevant laws. As this argument is rather new and not yet discussed broadly in legal writing, to be conservative, we for the time being give a relatively low probability to succeed.</i>
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request ¹⁴⁾	0%	100.00%	<i>For data stored in Switzerland we would expect this argument to work because a foreign lawful access would have criminal consequences for those involved, but in the case of customer data stored in Ireland, the resulting violation of the GDPR would in our view not deter the US government from accessing it.</i>
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case ¹⁵⁾	0%	100.00%	<i>n/a</i>
b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts? ¹⁶⁾	Yes	100.00%	<i>This is a requirement under the EU SCC entered into with the parent company.</i>
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience? ¹⁷⁾ †††	5%	5.00%	<i>The processed data is the internal corporate data, by no means communications or transactions among third parties. This is not the target of data gathering under Section 702 FISA or EO 12.333. This is confirmed both by a report of the Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit.ly/3yeO7us), the NSA's comments (https://bit.ly/3dFahhk), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQB). These sources contain no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, we believe that the probability that the provider has or will receive a surveillance order with respect to our data during the period under consideration is very low.</i>
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	40%	40.00%	<i>We do not know the provider's software, but due to the encryption of our data, the agreement that our data will be stored exclusively in Europe (i.e. from the U.S. there is only remote access without local storage), the assumption that the provider's software on the data centers in Europe does not have any backdoors for such searches (this would violate European law and thus the contract), the fact that the audit reports also contain no references to such functions (although they would be relevant from a security perspective), we assume that it is unlikely that the provider with respect to the data relevant in the present case is technically capable of performing such a search with respect to our data (including the on-the-fly decryption of the data). It would have to adapt its software for this, which would be possible in principle, but is not required in such scenarios and would hardly be technically possible without being noticed (including by the auditors). Moreover, it would then be possible to react immediately, since this monitoring is not customer-specific and is fundamentally future-oriented. In addition, the provider would have to adapt its contracts in order not to expose itself to the accusation of breach of contract; in our case, the provider obviously does not expect the</i>
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		<i>We are regularly monitoring the legal development in this area (and at least annually). Also, we have agreed with the data importer to regularly report on its experience with lawful access requests.</i>
Probability that legal arguments fail to prevent foreign lawful access: †††			19.20%	

Overall probability of a lawful access prohibited under applicable data protection laws:	0.38%	during the assessment period
In view of the TIA parameters, the residual risk of prohibited lawful access is:		
acceptable		
Number of years it takes for a lawful access to occur at least once with a 90 percent probability:	2,992	
Number of years it takes for a lawful access to occur at least once with a 50 percent probability:	901	
... assuming that the probability neither increases nor decreases over time (like tossing a coin)		

We have made the assesement in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics):

With the help of experienced outside counsel and legal research, as indicated

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is:	permitted	Reassess at the latest by:	1-Sep-26
--	-----------	----------------------------	----------

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:		Place, Date:	
Willy Beachum, Legal Counsel, ACME US Inc.; Angela Bennett, Data Protection Officer, ACME Europe Ltd.; Mitch McDeere, Bendini, Lambert & Locke (outside counsel); Alice Pleasance Liddell, Head of HR, ACME US Inc.		Signed:	
Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.		By:	

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks *only for the purposes of European data protection law*, where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where *any foreign lawful access is an issue*, for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at [www.rosenthal.ch](https://bit.ly/2V9dj7V) (<https://bit.ly/2V9dj7V>), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schrems II" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).

†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) *possibility* of it occurring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.

††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)

¹⁾ The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.

<p>²⁾ The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.</p>
<p>³⁾ Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.</p>
<p>⁴⁾ We have seen that many people have difficulties in coming up with a percentage figure for a probability of an event at which they "have no reason to believe" that it will occur (which is the test under the EU SCC and the EDPB guidance for the residual risk of a prohibited foreign lawful access). We also found that people are more comfortable in assessing the probability of an event by expressing its probability of occurring in number of years ("an earthquake of this kind is to happen only once in 100 years on average"). We, therefore, use this concept to calculate the "permitted" residual risk in percent. Because we are not assessing earthquakes (which happen in any event) we have set the benchmark at a 50% chance of a lawful access occurring. You can also use another value, but we believe that if a lawful access has a 50:50 chance of occurring it in our view has become an unacceptable risk. If it, however, takes a long period of time (for example an additional 30 years after our assessment period) for the chances to raise to that level (at which a lawful access is still far from certain statistically), many will conclude that the risk of it happening in the first (for example) five years of our assessment period is rather theoretical. We then, based on a statistics formula, calculate the acceptable percentage value for our assessment period (which is then used in Step 4, if necessary).</p>
<p>⁵⁾ You do not have to use our "50:50 chances"-method of determining the maximum percentage for assessing the probability of lawful access that results from Step 4. If you wish, you can manually enter the percentage figure you think is still acceptable (thus overwriting the formula in the cell). The grey number on the right hand of the percentage figure will tell you what this will mean in terms of years when using our method. If you do not manually overwrite the percentage, you can ignore the grey number.</p>
<p>⁶⁾ You will normally not need to care about this figure. It becomes necessary if the importer does not have a "defend you data" obligation, i.e. is not obliged to challenge lawful access requests in its own jurisdiction. In these cases, we use this figure to determine the probability of the authorities obeying the law even if their lawful access requests are not challenged by the importer (if the importer does challenge the lawful access request, a court or other authority will usually determine whether the legal prerequisites for the lawful access are met). A value of 50% means that in half of the cases the authorities may issue and try to enforce a lawful access request even if the requirements of law are not met. If that happens, the assessment in Step 4 becomes partially moot, because it is based on the assumption that a lawful access will be successful only if the prerequisites set forth by law are met. With this figure we take this uncertainty into account if the importeur is expected not to make sure that lawful access requests are challenged.</p>
<p>⁷⁾ This question is, in principle, not necessary for assessing the transfer. We have nevertheless included it because many data protection authorities will want to know whether the exporter has considered alternatives to transferring personal data into a non-whitelisted country and why they are not pursued. The response has no impact on the outcome of the assessment but is for mere documentary purposes.</p>
<p>⁸⁾ This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).</p>
<p>⁹⁾ In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered <i>not</i> fulfilling in particular requirement (3) and (4). Hence, it has to be verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.</p>
<p>¹⁰⁾ Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at https://bit.ly/3rSv070), the FAQ for company of NOYB (including forms to be sent to US providers, available at https://bit.ly/2Vozeb7), the Swiss Federal Data Protection and Information Commissioner's guidance (available at https://bit.ly/37b5tHs), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.</p>
<p>¹¹⁾ Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "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." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (https://bit.ly/3lgsTt5).</p>
<p>¹²⁾ For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (https://bit.ly/3l2xfC9). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) with a summary of the standards of US law as to what amounts to "control".</p>
<p>¹³⁾ According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at https://bit.ly/3qHNMy7 and a full paper from the same author at https://bit.ly/2V9veez with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at https://bit.ly/3l12oHZ.</p>
<p>¹⁴⁾ The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://bit.ly/3eVzLSq).</p>
<p>¹⁵⁾ An example could be the following case: The importer uses a piece of software for managing the data, which is technically not able to comply with a lawful access request (e.g., a CRM or ERP software with a proprietary database structure), but could be amended to do so. However, in the specific case, doing so would violate copyright law because the importer has no right to change the software or not the necessary information to do so. If this circumstance is not considered above in connection with having "control" over the data at issue or below as a technical barrier, it can be considered here as another (legal) obstacle towards compliance with the lawful access request.</p>

¹⁶⁾ The legal arguments above are useless if it is not ensured that they are complied with in case of a specific lawful access request. This can be ensured by the importer challenging such requests (which, in turn, can be secured by having a corresponding "defend your data" clause in the contract, which the EU SCC have). If there is no such obligation to challenge such requests, the exporter will depend on the probability of the authorities at issue to comply with their own law, which is usually below 100%. The relevant percentage is taken from Step 2 and applied to the overall calculation.

¹⁷⁾ Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the *categories* of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLOB) (<https://bit.ly/3yeO7us>), the NSA's comments (<https://bit.ly/3dFalkh>), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: <https://bit.ly/3heBYQB>). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).

* This form and the underlying method was developed by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP), Baltasar Cevc (Fingolex), Katharina Koerner, David Vasella (WalderWyss), Josh Edgerly (IAPP) and others. David Rosenthal can be reached at david@rosenthal.ch (private) or drosenthal@vischer.com (office).

DISCLAIMER: You are using of this spreadsheet and transfer impact assessment method on an "as is" basis without any implied or express warranties, and entirely at your own risk, as it may contain errors. It provided you for informational purposes only and does not replace getting professional legal advice. Please report me any errors you find or other thoughts you have, so that I can update the file. See also my original work on the topic (incl. a scientific paper in German), which is available at <http://www.rosenthal.ch> and the Excel specifically at https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

All rights in this spreadsheet and transfer impact assessment method are reserved. This file is made available under a free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license (<https://creativecommons.org/licenses/by-sa/4.0/>). The input fields (blue background) and sample text therein are not subject to the license and may be changed and shared. Attribution must also include reference to the link where the original and master version of this file can be obtained at www.rosenthal.ch. If you need a different license, contact me at david@rosenthal.ch.



EU SCC Transfer Impact Assessment (TIA)



If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

Author: David Rosenthal (original version at www.rosenthal.ch)*
(Licensing: See bottom)

Version 1.01 (September 1st, 2021)

(Version for transfers to USA)

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The **green text** is mere sample text; the values and reasoning do *not* necessarily represent the author's opinion and are given for illustration purposes only.

Step 1: Describe the intended transfer

a)	Data exporter ¹⁾ (or the sender in case of a relevant onward transfer):	SocialMediaCorp Europe Operations Limited	
b)	Country of data exporter:	Ireland	
c)	Data importer ²⁾ (or the recipient in case of a relevant onward transfer):	SocialMediaCorp Inc.	
d)	Country of data importer:	USA	
e)	Context and purpose of the transfer:	Hosting, Technical Support and End User Support/Management	
f)	Categories of data subjects concerned:	User data, third parties included in user content	
g)	Categories of personal data transferred:	User content, user communications, usage data, user profile data	
h)	Sensitive personal data:	All special categories of data are in principle possible	
i)	Technical implementation of the transfer:	Mirroring of user content and user content to US servers, remote access to usage data and user profile data	
j)	Technical and organizational measures in place (optional):	IGDTA, individual access control on need-to-know-basis, encryption in-transit & at-rest, data loss prevention and endpoint protection systems, NDAs, instructions, trainings and audits (for more, see IGDTA)	
k)	Relevant onward transfer(s) of personal data (if any): ³⁾	None	→ perform separate TIA
l)	Countries of recipients of relevant onward transfer(s):	None	

Step 2: Define the TIA parameters

Reasoning				
a)	Starting date of the transfer:	1-Sep-21		
b)	Assessment period in years:	5		Once we approach the end of the period, we will re-assess the situation.
	Ending date of the assessment based on the above:	1-Sep-26		
c)	Determining the acceptable residual risk of foreign lawful access: If the probability of a lawful access happening in the assessment period is so low that the chances of it are still only at 50:50 if another xx years were to pass by, then the probability of it happening in the initial period is so low that we have no reason to believe that it will occur in such period. What should xx be? ⁴⁾	30	(= in total 35 years)	We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.
	Probability permitted calculated based on the above (alternatively, you can manually override this value ⁵⁾):	9.43%	30	
d)	Target jurisdiction for which the TIA is made:	USA		(if there are additional jurisdictions, perform a separate TIA)
e)	Relevant local laws taken into consideration:	Section 702 FISA, EO 12.333 (and PPD-28)		
f)	In how many cases will authorities in the target jurisdiction comply with their laws when pursuing lawful access even if not challenged? ⁶⁾	50%		This value is not relevant in our case. We have left it unchanged.

Step 3: Define the safeguards in place

Reasoning				
-----------	--	--	--	--

a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? ⁷⁾	No		Given our operational structure, there is no alternative to have the personal data at issue also processed in the US.
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		n/a
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? ⁸⁾	No	Ensure that data remains encrypted	All traffic over telecom lines is protected by state-of-the-art line encryption (VPN).
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign lawful access is at least technically possible	The recipient needs access to the data in clear text in order to be able to process it. Encryption is not possible.
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	Ensure that the mechanism remains in place and is complied with	We have in place an IGDTA based on the new EU SCC, and we have no reason to believe that the data importer will not comply with them, to the extent that US law permits so. Regular audits confirm the adequacy of the data security agreed therein.
Based on the answers given above, the transfer is:		permitted, subject to Step 4		

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction⁹⁾

Country-specific! The following factors have been drafted for **US law**; amend as necessary for other jurisdictions.

a)	Assess the probability that during the assessment period, the following <i>legal arguments</i> will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in Step 2 above: ¹⁰⁾			
		Probability†	Probability of possibility of a (successful) request‡	Reasoning
	The data importer/recipient is no "Electronic Communications Service Provider" ¹¹⁾ with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	10%	90.00%	We may argue that the data importer does, in fact, not provide any services to the end user, as this is done by the subsidiary in Europe. However, even in this case, the type of service is the service typically provided by an ECSP.
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws ¹²⁾	10%	90.00%	The data importer does have, in fact, possession or custody of personal data of the European subsidiary, as it is transferred to the US. It will likely be considered having control over the data that is remotely accessible.
	The transfer of the personal data at issue or the content of the personal data will be considered communications to either a person located in the United States or a US person, which may not be "intentionally targeted" by the US authorities under the relevant laws, but such targeting would occur in the present case, and, thus, prevent such a request ¹³⁾	10%	90.00%	The data importer is a US person, and the data at issue is sent to such company. However, it contain communications that was never targeted to a US person and not intended to be sent to the US. It would amount to a circumvention of Section 702 FISA if one were to refuse compliance with a search order for such non-US communications by having it first transferred to the US.
	Performing a prohibited lawful access would violate the data exporter's or other applicable foreign law in a manner that is not permitted under the US law doctrine of international comity, which, thus, prevents such a request ¹⁴⁾	30%	70.00%	The access may, indeed, violate European data protection law, but it is not very likely that the US authorities will consider this as sufficient grounds not to order access such data.
	There are other legal grounds under US law that prevent a prohibited lawful access to occur in the present case ¹⁵⁾	0%	100.00%	n/a

b)	Is the data importer/recipient contractually required to defend the personal data at issue against lawful access attempts? ¹⁶⁾	Yes	100.00%	<i>This is a requirement under the EU SCC entered into with the data importer.</i>
c)	Probability that during the assessment period, the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience? ¹⁷⁾ †††	100%	100.00%	<i>At least the user communications is typically the type of information that is searched for under Section 702 FISA, although we so far did not have such requests.</i>
d)	Probability that during the assessment period, the data importer/recipient is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws? †††	100%	100.00%	<i>The data importer does have access to the data in a form that can be searched.</i>
f)	Are measures in place to find out if during the assessment period the circumstances taken into account in the above assessments are no longer valid?	Yes		<i>We are regularly monitoring the legal development in this area (and at least annually). Also, we have agreed with the data importer to regularly report on its experience with lawful access requests.</i>
Probability that legal arguments fail to prevent foreign lawful access: †††			51.03%	} during the assessment period
Overall probability of a lawful access prohibited under applicable data protection laws:			51.03%	
In view of the TIA parameters, the residual risk of prohibited lawful access is:		not acceptable		
Number of years it takes for a lawful access to occur at least once with a 90 percent probability:		16		
Number of years it takes for a lawful access to occur at least once with a 50 percent probability:		5		
... assuming that the probability neither increases nor decreases over time (like tossing a coin)				
We have made the assesement in Step 4 on the following basis (e.g., internal legal analysis, outside legal advice, support by the data importer, legal research, public documentation, statistics):		With the help of experienced outside counsel and legal research, as indicated		
Final Step: Conclusion				
In view of the above and the applicable data protection laws, the transfer is:		not permitted		
This Transfer Impact Assessment has been made by:		Place, Date:		
Moritz Schrams, outside counsel		Signed:		
Note: Under the EU SCC, the TIA is to be adopted by both the data exporter and importer.		By:		

Scope of this TIA: This Transfer Impact Assessment should be used for assessing foreign lawful access risks *only for the purposes of European data protection law*, where foreign lawful access is not per se a problem, but only if it does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. Accordingly, foreign lawful access requests that can be challenged before an independent and impartial court (in a European sense of the word) are permitted if they are regulated by law, are needed to safeguard the aforementioned objectives (such as prosecuting crimes), are undertaken in a proportionate manner and come with the possibility of the data subject getting legal redress. For instance, lawful access by way of the US CLOUD Act is in principle not an issue under European data protection law; in fact, it is in line with the Cybercrime Convention of the European Council. That said, there may be cross-border transfers of data where *any foreign lawful access is an issue*, for example, in where professional secrecy obligations apply. In such cases please use the spreadsheet "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" also from David Rosenthal, available at www.rosenthal.ch (<https://bit.ly/2V9dj7V>), which provides for a risk assessment also for these types of foreign lawful access. In turn, this TIA focuses on foreign lawful access where there is no possibility for recourse to an independent court, which is what has been the issue in the "Schrems II" decision by the European Court of Justice in its decision C-311/18 of July 16, 2020.

Legal Basis of this TIA: Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021), Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

† Example: If you believe that a particular legal argument will be found valid by three out of ten judges assessing the same case, the probability will be 30%. If you conclude that the argument is not valid, enter 0%. If you believe it will in any event be successful, put in 100%. If you don't know, put in 0%. Of course, nobody can predict the future, but this is also not necessary. For a TIA it is sufficient to undertake an diligent and professional predictive judgement following a proper protocol. To avoid noise and bias, we have already split up and structured the assessment in several independent parts. To further reduce noise and bias, ask several knowledgeable people to independently provide their assessment, then have them discuss their values, and then ask them to again provide their assessment. Use the average of the values each of them provided after the discussion (this referred to as the "Delphi" method).

†† In line of the recommendations of the EDPB, we do not assess whether the access will actually occur or not (because they are not interested in the company XY or their employees). We assess the (objective) *possibility* of it occurring. A 100% possibility means that we have to expect that a lawful access under the relevant laws will occur during the period, but it may still not happen because the relevant authorities do not believe it makes sense to order the data importer to produce the data at issue given their specific tasks, projects, etc. which we don't know about.

††† These values correspond to the values in C50, C52 and C51 of the "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" spreadsheet (available on www.rosenthal.ch)

¹⁾ The data exporter is the party being subject to the GDPR or Swiss DPA who exports personal data to a non-whitelisted third country (e.g., the US). It has the same meaning as in the EU Standard Contractual Clauses (SCC). The data exporter can be a controller, joint controller, processor or sub-processor. It is not relevant whether the data exporter is itself in Europe, a whitelisted country or a non-whitelisted country. It will always be required under the EU SCC and GDPR or Swiss DPA to perform a TIA. If the TIA is performed for the purpose of assessing a relevant onward transfer then the sender or originator of the relevant onward transfer is the "data exporter" for the purposes of this TIA.

²⁾ The data importer is the party in a non-whitelisted country (e.g., the US) who receives personal data from a data exporter. The data importer can be a controller, joint controller, processor or sub-processor. It is the party with whom the data exporter will typically want to enter into the EU SCC (unless there are other grounds for the transfer). If the TIA is performed for the purpose of assessing a relevant onward transfer then the recipient of the relevant onward transfer is the "data importer" for the purposes of this TIA.

³⁾ Relevant onward transfers of personal data are onward transfers of personal data by a data importer to another party in a non-whitelisted country. If this other party is a processor or sub-processor, even if the data exporter has no direct contractual relationship with it, a separate TIA has to be performed for such relevant onward transfer if the recipient is in a non-whitelisted country, because such relevant onward transfer can, as well, expose the personal data at issue to the risk of prohibited foreign lawful access. Since this TIA can be made for only one country and one recipient at a time, fill out and perform multiple TIAs for each recipient of a relevant onward transfer.

⁴⁾ We have seen that many people have difficulties in coming up with a percentage figure for a probability of an event at which they "have no reason to believe" that it will occur (which is the test under the EU SCC and the EDPB guidance for the residual risk of a prohibited foreign lawful access). We also found that people are more comfortable in assessing the probability of an event by expressing its probability of occurring in number of years ("an earthquake of this kind is to happen only once in 100 years on average"). We, therefore, use this concept to calculate the "permitted" residual risk in percent. Because we are not assessing earthquakes (which happen in any event) we have set the benchmark at a 50% chance of a lawful access occurring. You can also use another value, but we believe that if a lawful access has a 50:50 chance of occurring it in our view has become an unacceptable risk. If it, however, takes a long period of time (for example an additional 30 years after our assessment period) for the chances to raise to that level (at which a lawful access is still far from certain statistically), many will conclude that the risk of it happening in the first (for example) five years of our assessment period is rather theoretical. We then, based on a statistics formula, calculate the acceptable percentage value for our assessment period (which is then used in Step 4, if necessary).

⁵⁾ You do not have to use our "50:50 chances"-method of determining the maximum percentage for assessing the probability of lawful access that results from Step 4. If you wish, you can manually enter the percentage figure you think is still acceptable (thus overwriting the formula in the cell). The grey number on the right hand of the percentage figure will tell you what this will mean in terms of years when using our method. If you do not manually overwrite the percentage, you can ignore the grey number.

⁶⁾ You will normally not need to care about this figure. It becomes necessary if the importer does not have a "defend you data" obligation, i.e. is not obliged to challenge lawful access requests in its own jurisdiction. In these cases, we use this figure to determine the probability of the authorities obeying the law even if their lawful access requests are not challenged by the importer (if the importer does challenge the lawful access request, a court or other authority will usually determine whether the legal prerequisites for the lawful access are met). A value of 50% means that in half of the cases the authorities may issue and try to enforce a lawful access request even if the requirements of law are not met. If that happens, the assessment in Step 4 becomes partially moot, because it is based on the assumption that a lawful access will be successful only if the prerequisites set forth by law are met. With this figure we take this uncertainty into account if the importeur is expected not to make sure that lawful access requests are challenged.

⁷⁾ This question is, in principle, not necessary for assessing the transfer. We have nevertheless included it because many data protection authorities will want to know whether the exporter has considered alternatives to transferring personal data into a non-whitelisted country and why they are not pursued. The response has no impact on the outcome of the assessment but is for mere documentary purposes.

⁸⁾ This is relevant for assessing the exposure to lawful interception of Internet backbones using selectors (upstream monitoring of communications).

⁹⁾ In this section, the probability of a foreign authority accessing the personal data in clear text in a manner that does not respect the essence of the fundamental rights and freedoms or exceeds what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. The analysis only has to assess provisions of the target jurisdiction that grant public authorities access to the personal data at issue and fail to, in essence, satisfy any of the following four requirements: (1) Access is subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) access is subject to the principle of proportionality, (3) there are effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access is subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). For example, in the US, access requests on the basis of Section 702 FISA (Foreign Intelligence Service Act) and EO 12.333 are considered *not* fulfilling in particular requirement (3) and (4). Hence, it has to be verified how probable it is that there may be access requests on the basis of these two legal grounds. If the probability is so low that the exporter has "no reason to believe" that such access will occur, the transfer is permitted as per the SCC, the GDPR and the CH DPA, even though the SCC or BCR as such would not provide protection against such requests. The analysis in this section shall be based on the law applicable in the target jurisdiction and the way how it is applied by authorities and courts (including court decisions). The analysis may require obtaining a legal opinion or other forms of legal advice from counsel.

¹⁰⁾ Consider all documented information on applicable legislation, case law, practices of authorities and past experience (including of the data importer, where available). You may want to ask the data importer the necessary questions (Clause 14(c) actually requires the data importer to provide "relevant information"). On this topic, see, for the EDPB recommendations 01/2020 on supplementary measures (version 2.0 adopted on May 18, 2021, available at <https://bit.ly/3r5v070>), the FAQ for company of NOYB (including forms to be sent to US providers, available at <https://bit.ly/2Vozeb7>), the Swiss Federal Data Protection and Information Commissioner's guidance (available at <https://bit.ly/37b5tHs>), and private publications, such as for example, Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at <https://bit.ly/3qHNMy7> and a full paper from the same author at <https://bit.ly/2V9veez> with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at <https://bit.ly/3l12oHZ>.

¹¹⁾ Under U.S. law, the term is broadly understood under Section 702 FISA; it includes telcos, ISPs, email providers, cloud services and "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." This also covers social media providers and may even include all companies that otherwise provide their users with the ability to send or receive electronic communications; theoretically, this also includes companies that provide e-mail services to their employees (even if only for business purposes). NOYB provides a form to ask service providers whether they are ECSPs (<https://bit.ly/3lgsTt5>).

¹²⁾ For a discussion of the term "possession, custody, or control" see, for example, Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 of January 23, 2020 (<https://bit.ly/3i2xfC9>). Control may exist either in the form of "legal control" (the right to request access to the data in a particular situation) or "day-to-day control" (the ability to access data in day-to-day business). See also Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (<https://bit.ly/3rLQfbp>) with a summary of the standards of US law as to what amounts to "control".

¹³⁾ According to Section 702, 50 U.S.C. 1881a(b), the US authorities "may not intentionally target" "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." A "United States person" (or "US person") is anybody who is a (i) citizen or national of the US, (ii) an alien lawfully admitted for permanent residence (e.g., green card holder), (iii) an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence or (iv) a corporation that is incorporated in the US (<https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4>). See on this argument Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", December 21, 2020, available at <https://bit.ly/3qHNMy7> and a full paper from the same author at <https://bit.ly/2V9veez> with the follow-up post "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, available at <https://bit.ly/3l12oHZ>.

¹⁴⁾ The doctrine of international comity, as recognized under US law, provides certain standards or rules in resolving conflicts between US and foreign laws. See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (<https://bit.ly/3eVzLSq>).

¹⁵⁾ An example could be the following case: The importer uses a piece of software for managing the data, which is technically not able to comply with a lawful access request (e.g., a CRM or ERP software with a proprietary database structure), but could be amended to do so. However, in the specific case, doing so would violate copyright law because the importer has no right to change the software or not the necessary information to do so. If this circumstance is not considered above in connection with having "control" over the data at issue or below as a technical barrier, it can be considered here as another (legal) obstacle towards compliance with the lawful access request.

¹⁶⁾ The legal arguments above are useless if it is not ensured that they are complied with in case of a specific lawful access request. This can be ensured by the importer challenging such requests (which, in turn, can be secured by having a corresponding "defend your data" clause in the contract, which the EU SCC have). If there is no such obligation to challenge such requests, the exporter will depend on the probability of the authorities at issue to comply with their own law, which is usually below 100%. The relevant percentage is taken from Step 2 and applied to the overall calculation.

¹⁷⁾ Here, we do not assess whether the authorities will be interested in the data of the particular data exporter at issue (e.g. company XY and its employees = subjective view), but whether the *categories* of personal data at issue are, based on the practices of the relevant authorities, the subject of their lawful accesses at issue, either because such data is the target or because it is a by-catch (= objective view). Do not consider legal arguments here, as they are considered under a) (otherwise this results in double-counting). This may not be easy to assess at first sight, but there are sources available, such as the official reports that discuss the monitoring by the relevant authorities. See, for example, the Privacy and Civil Liberty Oversight Board (PCLOB) (<https://bit.ly/3yeO7us>), the NSA's comments (<https://bit.ly/3dFalkh>), and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: <https://bit.ly/3heBYQB>). Also consider the past experience of the data importer, where available (even if not substantiated by independent reports; the inexistence of such requests to the data importer as such does not mean that the probability is 0%, though; depending on the circumstances, the inexistence may just be coincidence).

* This form and the underlying method was developed by David Rosenthal, VISCHER (Switzerland), with the contribution of Samira Studer (VISCHER). Thanks for valuable input to Caitlin Fennessy (IAPP), Baltasar Cevc (Fingolex), Katharina Koerner, David Vasella (WalderWyss), Josh Edgerly (IAPP) and others. David Rosenthal can be reached at david@rosenthal.ch (private) or drosenthal@vischer.com (office).

DISCLAIMER: You are using of this spreadsheet and transfer impact assessment method on an "as is" basis without any implied or express warranties, and entirely at your own risk, as it may contain errors. It provided you for informational purposes only and does not replace getting professional legal advice. Please report me any errors you find or other thoughts you have, so that I can update the file. See also my original work on the topic (incl. a scientific paper in German), which is available at <http://www.rosenthal.ch> and the Excel specifically at https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

All rights in this spreadsheet and transfer impact assessment method are reserved. This file is made available under a free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license (<https://creativecommons.org/licenses/by-sa/4.0/>). The input fields (blue background) and sample text therein are not subject to the license and may be changed and shared. Attribution must also include reference to the link where the original and master version of this file can be obtained at www.rosenthal.ch. If you need a different license, contact me at david@rosenthal.ch.



Instruction on how to fill out this TIA

- Check **whether you need a TIA** and who is responsible to perform it (see worksheet "TIA Scenarios"). This TIA is *not* intended for transfers among parties in the EEA and whitelisted countries. Also check, whether the personal data transferred is subject to additional restrictions (such as professional secrecy obligations) that may require an assessment of additional risks of foreign lawful access than required when using the EU SCC (in such cases, see our separate Excel at <https://bit.ly/2V9dj7V>).
- In **Step 1** you should describe the transfer at issue. Perform a separate TIA for each transfer, i.e. if there are onward transfers that occur following the original transfer (e.g., from a controller to a processor), then complete a separate TIA for these other transfers. The reason is that each transfer has its own risk profile. However, you only need to perform one TIA if there are several transfers that have the same risk profile (e.g., several group companies that transfer the same kind of personal data for the same purposes to the same parent company in the US). None of the fields in Step 1 are used for the assessment math below; they are for documentation purposes only.
- In **Step 2**, enter the starting date and number of years for which the TIA is to be made. You should always limit the assessment for a reasonable period of time. You can't in a meaningful manner assess the risk for the next hundred years. The number is relevant for calculating the probability of lawful access you are willing to accept. The period of time is the time for which the data importer will have access to the personal data. After that period, a new TIA has to be made, and, depending on the outcome, the data may continue to remain in the hands of the data importer or the EU SCC have to be terminated and the personal data deleted by the importer.
- In **Line 23**, enter a number of years. This parameter helps you to determine which probability is acceptable under the EU SCC in order to conclude that you have no reason to believe that a prohibited lawful will occur during the assessment period (i.e. the number in Line 21). Try to imagine of how low the probability of the event (here: a successful lawful access) must be during the assessment period for you to qualify it as being a merely "theoretical" event. Because coming up with a meaningful percentage figure is difficult for most of us, we use a different formula: We all agree that if the chances of the event occurring during the five year assessment period are 50 percent, then the event is not theoretical at all. However, if the chances of the event are so low that an additional 30 years (on top of the initial five) need to pass by for the chances to rise to 50 percent (assuming the probability does neither increase nor decrease over time, like when tossing a coin), most of us would probably consider the chances of the event occurring during the (initial) five years is, indeed, most unlikely if not theoretical. In such a case, put in the number 30, and the spreadsheet will in Line 24 calculate the probability that is acceptable for the assessment period by these standards. This will be used for determining the acceptable risk in Step 4. Of course, based on the foregoing logic, the number in Line 23 must be considerable higher than the one in Line 21 in order to make sense. See also the footnote. If you do not like this method of determining the permitted probability, you can also simply enter into the percentage value you are happy with in Line 24, thus overwriting the calculated figure (the number on the right will tell you which number of years you have to fill in in Line 23 for the documentation to be consistent; see also the footnote).
- In **Line 26** put in the laws of the target jurisdiction that are considered substandard from the GDPR's and the EU SCC's perspective, i.e. those laws that allow a lawful access that does not respect the essence of the fundamental rights and freedoms or *exceeds* what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR. For the US, the European Court of Justice in its "Schrems II" decision found that this is the case with Section 702 FISA and EO 12.333. For other non-whitelisted countries, you will have to get the advice from local counsel as to which laws may be relevant.
- In **Line 27**, you only have to include a value if the data importer has no obligation to "defend" your data against the lawful access attempts assessed by this TIA (otherwise you can enter any number). If you conclude the EU SCC, such an obligation will exist. The "defend your data" obligation is necessary to make sure that lawful access requests indeed follow the law. If the obligation does not exist, you can include the probability that the authorities will nevertheless follow the law. This will then be taken into account in Step 4. See also the footnote.
- In **Step 3** we ask you to answer a number of "Yes/No" questions to better assess the overall risk of lawful access. Depending on the response, it is already clear from the outset that there is no risk of the prohibit lawful access occurring (in particular if the personal data remains encrypted all the time). Conversely, there are situations where it is clear that the risk is (normally) too high (for example, if personal data is not encrypted in transit when being communicated over the Internet (where it can be easily picked up by upstream monitoring of Internet backbones). Also, in Line 41 you have to state whether the EU SCC (or another safeguard permitted under Art. 46 GDPR) is used; in the case of an onward transfer (e.g., if a processor in a non-whitelisted country onward transfers the data to a sub-processor in the same country, the EU SCC permit, for instance, the use of the EU SCC or another back-to-back contract). Of course, if you transfer data under one of the accepted exemptions of Art. 49 GDPR, no further assessments are necessary. If you encrypt data in transit, have the EU SCC in place, but can't prevent the data importer (in the non-whitelisted country) from accessing the personal data in clear text, you have to do a case-specific risk analysis, which is done in Step 4. Note that the answer in Line 30 will not effect the outcome of the TIA, but we have included it to remind you to think of the possibility of not transferring personal data to a non-whitelisted country in the first place, but instead use a solution relying exclusively on a data processing in the EEA or whitelisted countries.
- **Step 4** becomes necessary if you need to understand whether you will be facing a relevant risk of a prohibited lawful access in the country of the data importer. This is usually the most problematic and difficult part of a TIA. We have developed a new, math-based method to solve this problem. The unique feature of our TIA is that you do *not* have to be sure about the assessments you make when completing the form, and that you can work with rough figures. The method is also agnostic of whether you believe that lawful access concerns are warranted or not or that you find particular arguments used to prevent such access convincing. Also, the method has been structured to reduce noise and bias in order to get better judgements. We believe that it has clear advantages over the classical approach of only getting a legal opinion. You may still need and want to get a legal opinion to do the TIA, but with our method, you get much clearer results that factor-in the uncertainties any legal opinion will come with. The way how this is achieved is that we rely on probability calculations and a structured approach combining both legal, technical and factual elements. While the approach does not allow us to predict the future (nobody can), such methods are well accepted for assessing risks - which is what a TIA is all about. Note that the current content of Step 4 has been drafted with **US law** in mind. For other jurisdictions, different content is necessary. Over time, we or other sources may provide further content for Step 4. Also note that the Excel will automatically "fade out" Step 4 if, based on the other responses, it is not necessary to complete.
- You may want to fill-out Step 4 in workshop with a group of people. If you do so, you can make use of the **Delphi method**. We have already included a section that will help you do so on the right hand side of the TIA, including a short instruction on how to use it. The Delphi method aims to improve decision making in groups of people by reducing noise and bias. You can delete the table we have

Delphi method aims to improve decision making in groups of people by reducing noise and bias. You can delete the table we have created for the Delphi method once you have used it or if you do not want to use it.

- In **Lines 41-45** we ask you to assess how probable it is that each of these legal arguments will prevent a prohibited lawful access in your particular case. The arguments are either prerequisites that need to be fulfilled for a lawful access to occur, or they are arguments to otherwise stop such access from happening. Depending on your case and your opinion, you may reach your own conclusion on how probable these arguments will be successful. For instance, if you believe that the "intentionally target" argument (as developed by Alan Raul, see the footnote) is convincing, you may in a particular situation give it a high percentage; if you don't believe so, you may give a low probability. If a particular argument will, in your opinion, not work at all in the scenario at hand, give it a 0% percent chance. If you think that an argument will in any event prevent access, give it a 100%. However, you will usually tend to give more balanced judgements, considering the fact that there may be different views on the argument by the relevant decision makers. If you believe that four out of ten of them will buy into a particular argument, then put in 40%. In other words: You do not have to be sure about an argument; you can work with probabilities, and it is not necessary to be precise. The method will work fine even with very rough figures.
- **Line 47** is usually a "Yes" if you use the EU SCC, but if not (for instance in case of some older BCR), the math will result in an increase of the probability of foreign lawful access based on your assessment in Line 27 of whether the relevant authorities will nevertheless comply with their law.
- In **Line 49**, you are asked to make an assessment of the probability that the type of personal data at issue is targeted by the relevant authorities when performing the prohibited lawful access exercises. Here, we need to distinguish carefully: We are not asking you to assess how much the authorities may be interested in *your* data, i.e. the data of your company, your employees, your customers, etc. Such a *subjective* assessment is not a factor accepted by European data protection authorities. What you need to assess is how probable the category of data at issue is in general the target of access requests by the relevant authorities or a by-catch of such requests. This is an *objective* factor and, therefore, permissible. However, it should be backed-up in one way or another, to the extent reasonably possible. For example, there are several publications, decisions and reports that provide information as to what kind of data is captured in the context of the lawful access exercises at issue here (we have listed some of them in the corresponding footnote). Also, past experience of the data importer may be taken into account (but usually cannot be the only source, unless it is representative of the overall practice of the relevant authorities). Note that you should not consider in Line 48 any of the legal arguments you already assessed in Lines 41-45 to avoid double counting.
- In **Line 51**, you are asked to assess the technical ability of the data importer to fulfill the kind of requests that is made under the relevant laws. While the requests may differ from jurisdiction to jurisdiction, in the US they are about constant searching of data for certain keywords, i.e. not all data is collected. Depending on the specific case, it may not be possible for the data importer to perform such searches on the personal data at issue, for instance if the clear text access granted requires prior "release" by the data exporter. In these cases, the data importer will have access to clear text data, but not in a form usable for such searches. This may effectively prevent such data to be picked up even if a search order has been issued.
- In **Line 53**, please confirm that you have a measure in place that will warn you if the circumstances that you rely on for the assessment change during the assessment period. Without such a measure, you can't rely on the assessment and the transfer is automatically considered as too risky when using the Excel.
- The **Lines 55-63** will provide you with the "residual" risk of a prohibited lawful access occurring during the assessment period, calculated based on the assessments made by you. Whether it is acceptable or not depends on whether the probability is below the figure determined in Line 24, based on your assessment in Line 23 (see above). Keep in mind that the years in Line 61 and 62 are calculated on the assumption that the risk neither increases nor decreases over time. Therefore, do not perform such assessments on

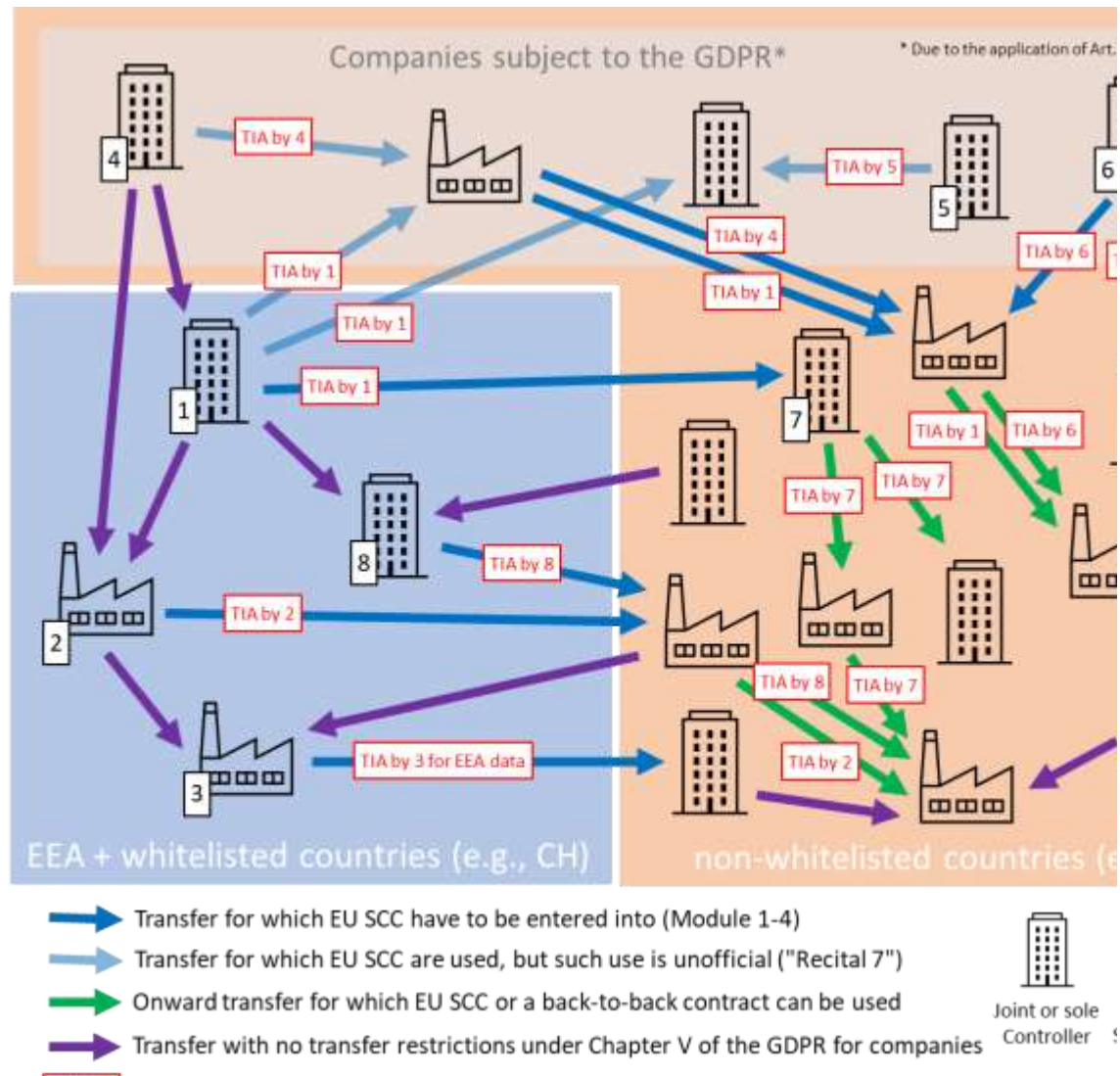
In which cases do you need to perform a TIA?


The EU Standard Contractual Clauses (SCC) require that a Transfer Impact Assessment (TIA) is performed before entering into, as the parties can otherwise not give the warranties provided for in Clause 14(a)-(d), i.e. that they believe that the laws and practices in the third country of destination applicable to the processing of the data importer prevent the data importer from fulfilling its obligations under the Clauses, and they shall do an assessment made to reach such conclusion.

This, however, is not the entire picture. A TIA does not only have to be performed for the transfer to the (original) controller of personal data in a non-whitelisted third country. A TIA will usually also have to be performed before under transfers of the personal data to other recipients in non-whitelisted third countries:

- If the onward transfer is still part of a processing for the (original) controller, that controller will be responsible for performing such TIA, as it remains responsible for the protection of "its" personal data along the chain of processing, even if the onward transfer is not done by itself (but by its processor or sub-processor).
- If the onward transfer is undertaken by a controller (as the initial recipient) to another controller or processor (or a further transferring) controller is responsible to comply with the provision on onward transfers in the new SCC. If the exceptions in the new SCC apply, the controller will have to itself enter into the new SCCs or a back-to-back contract to ensure continued protection of the personal data during the onward transfer (as stated above). As part of this, the controller will also have to perform a TIA.

The following chart illustrates the various scenarios in which a TIA becomes necessary:



 Indicates that a Transfer Impact Assessment needs to be made and the primarily responsible p

For more information see the **FAQ on the EU SCC** at <https://www.rosenthal.ch/downloads/VISCHER-faq-s-VISCHER>).

If you need an **extended lawful access analysis** covering also foreign lawful access scenarios (e.g., US CLC principle not an issue under the GDPR, but may violate professional secrecy obligations, see https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx).

Some more useful resources when using the EU SCC:

- Graphical overview on which modules of the EU SCC to use (WalderWyss): <https://datenrecht.ch/wp-content/uploads/210726-Overview-constellations-SCC-EN-V020.pdf>
- SCC Generators:
 - European Essentials Guarantees Guide: <https://www.essentialguarantees.com/scc>
 - TaylorWessing: <https://www.taylorwessing.com/de/online-services/scc-generator>
 - Oppenhoff: <https://www.oppenhoff.eu/de/legaltech/scc-generator>
 - LauxLawyers: <https://www.lauxlawyers.ch/en/neue-eu-standardvertragsklausel>
- Downloadable versions (doc) of each EU SCC Module (IAPP): <https://iapp.org/resources/article/eu-standard-clauses-word-documents/>