

TOOLKIT

Road Map Transfer Impact Assessment



DPO Consultancy
Experts in Data Privacy

When your organization transfers personal data to countries outside the European Economic Area (EEA), it is important to ensure that the same level of protection, as provided in the Member States in the EEA, applies in these so called 'third countries'. For example, if you transfer personal data from Germany to the US, it is important that the same level of data protection also applies in the US.

Part of this legislation is that your organization always has a legal transfer mechanism for international data transfers. There are various transfer mechanisms, such as adequacy decisions, binding corporate rules and SCC. In practice, we see that for transfers to third countries, the Standard Contractual Clauses (SCC) is the most used transfer mechanism. Since September 27, 2021, when using this transfer mechanism, it is always mandatory to conduct a Transfer Impact Assessment (TIA) before the personal data is allowed to leave the European Economic Area.



Want to learn more about Standard Contract Clauses?
Watch our previous webinar on the new SCCs.



What is a TIA?

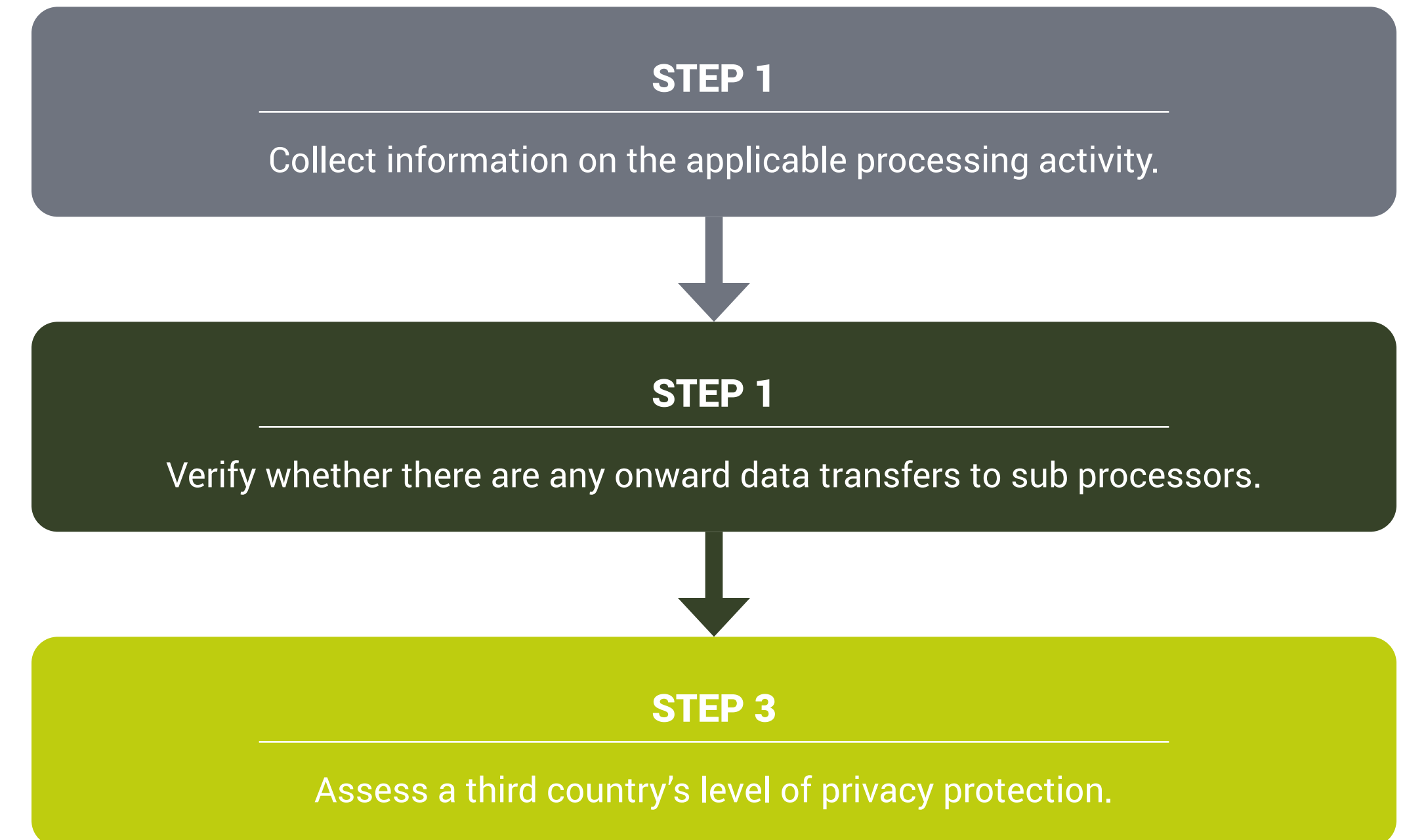
A Transfer Impact Assessment is a tool that enables your organization to assess the risks involved when sending data internationally. Currently, the TIA is form free, although the European Data Protection Board provided draft guidelines on how to conduct a TIA and what supplementary measures can be implemented to mitigate risks.

It is important to note that if the supervisory authority contacts either the data importer or the data exporter to review the TIA that has been conducted for the transfer, it must be provided. This is in line with the accountability principle under the GDPR that requires organizations to document their GDPR compliance.

How should you conduct a TIA?

With a Transfer Impact Assessment, it is important that your organization knows what steps you need to take and how to do it. With this step-by-step plan we help your organization to carry out a Transfer Impact Assessment. We will explain to you which steps you have to go through and what you should keep in mind when taking those steps. This way you can perform TIAs in a clear and responsible manner.

The three steps of the Transfer Impact Assessment



Step 1

Collect information on the applicable processing activity

There are many specific elements to review in this step, but the bottom line is that you need to describe the data journey to understand how the data moves from input to output. In addition, you must also describe the security of the data. What measures are there to protect the data? And finally, you need to answer the following six questions: who, what, when, where, why and how? These could be questions like:

- Who sends the data?
- What personal data is involved?
- When and how often does the transfer take place?
- Where is the data sent?
- Why is it necessary to send the data? What is the purpose?
- How is the data sent? What is the data format?

The basis for your TIA is that you have all the necessary information about the relevant processing activity. When you have data from processing activities to fall back on, the information you need for this step is easy to find. If not, you will need to collect important information about the processing activity.

Another scenario is that there may be an agreement that contains a lot of information that you can use as a source. Examples are Master Services Agreements, Data Processing Agreements and Distributor Agreements.

Step 2

Verify whether there are any onward data transfers to sub processors

After you have collected all information about the processing activity, it is necessary to assess whether there are onward data transfers to sub processors (a processor engaged by a processor). This is important because you could find that the data is sent to multiple third countries. You should be aware that as the controller of the processing activity you are responsible for confirming this with the processor and sub-processor.

Therefore, it is important to ask yourself the six questions, similar to step 1, regarding the onward transfers (if applicable): who, what, when, where, why, and how? At this step you can think of questions such as:


- Who is the processor and what sub processors are involved?
- What are the exact roles of the processor and sub processors?
- When must this deadline be met? Since you need to gather the information prior to the onward data transfer and before the SCCs are concluded.
- Where is the data stored?
- Considering data minimization, why is it necessary for the processor and sub processor to process this data?
- How are the contractual relations between the different parties arranged? Did you conclude SCC's, additional Data Processing Agreements, etcetera?

Step 3


Assess a third country's level of privacy protection

Finally, you should assess whether an authority requests disclosure or access to the data from the data importer. How does this third country's law then deal with this? We list the most important things to keep in mind:

- Organizations often forget that it is not only about the GDPR, but also about the right to privacy: a fundamental human right. It is therefore also important to assess how human rights and fundamental freedoms are respected in third countries.
- Your organization should also assess which privacy laws apply. For example, does the country have a privacy law? This will give you the necessary insights into how the country respects privacy rights.
- Assess how the legal redress is arranged for data subjects - individuals whose personal data is processed. For example, if you are an individual who lives in the EU and you want to take legal action against an organization in Brazil, is it possible to go to court?
- Also compare the concept and principles of the GDPR with the respective third country legislation. Think of GDPR principles, such as data minimization, purpose limitation, or transparency. But also dealing with the rights of data subjects, such as the right to be forgotten or the right to access.
- Assess how easy it is for government agencies to access personal data. Does a government agency need to obtain a court order to gain access, or can it simply ask or demand that the data be handed over?



There are many more elements to assess in the third country's law. If you want to learn more on the other elements, please watch our latest webinar on how to conduct Transfer Impact Assessments.

 **REPLAY**

Scoring the identified risks

A preferred way to identify privacy risks is to use a risk scoring model. There are several options when it comes to risk scoring models. One way to identify risks is to score both the probability and the impact of the risk from 1 to 5. With probability score, 1 means that the risk is very unlikely and 5 means that the risk is very likely. With the impact score you measure the severity of the risk, where 1 has a minor impact on the individuals involved, and 5 has a very serious impact on the individuals involved.

Chance	1	2	3	4	5
The probability of the risk occurring	Very unlikely	Improbable	Possible	Probable	Very likely
Impact	1	2	3	4	5
The impact (consequence) of the risk	Low impact	Limited impact	Significant impact	Serious impact	Very serious impact

You can then list all the identified privacy risks in the data transfer by describing the actual circumstances you found and then explaining the consequences this could have on the privacy of individuals. Then you can focus on what additional measures you can take to mitigate the privacy risks. Additional measures may include the use of anonymization and pseudonymization where possible. This was recommended by the European Data Protection Board.

No.	Risk	Origin	Chance (1-5)
1	Based on the fact that.... (describe fact), there is a chance that (describe consequence)	Article 5(1)(b) GDPR; Purpose limitation	2
2		Article 5(1)(b) GDPR; Purpose limitation	2
3		Article 5(1)(b), (c), (d), (f) GDPR; purpose limitation, data minimization, accurate, integrity	3

Furthermore, additional measures or mitigating measures that your organization takes must show whether the residual risk is accepted, who owns that risk and when the measure will be completed. And in the end, a CEO opt-out is recommended, as it indicates the responsibility of the controller.

Risk no.	Measures	Residual risk	Residual risk accepted	Owner	Deadline
1					
2					
3					

Conclusion

Having gathered all the information on the processing activity, onward transfers to sub processors, and the level of privacy protection in the third country, you are able to identify privacy risks. With a Transfer Impact Assessment you ensure the same level of protection when your organization transfers personal data to countries outside the European Economic Area. This way you not only comply with laws and regulations, but you also prevent that you only notice possible problems afterwards.

**Do you have any additional questions about
the TIA or other specific topics?**
**Please contact us via info@dpoconsultancy.nl
or **+31 85 0711080****

Australiëlaan 12a
5232 BB 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

1 Lyric Square London
W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com

