PRACTICAL GUIDE

TRANSFER IMPACT ASSESSMENT

Final version

January 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table of contents

1. Introduction

1.1 Background

Regardless of their status (public or private, profit-making or non-profit) and their size (multinational or small and medium-sized enterprises, local or central administrations, artisans or liberal professions), a very large number of data controllers and data processors are concerned by the issue of data transfers outside the European Economic Area[1] (EEA). The interpenetration of networks and the development of cross-border services, in particular with cloud computing, have multiplied the situations in which personal data (hereinafter sometimes referred to simply as "data") are processed in whole or in part in third countries which are not subject to EU law. These situations may thus give rise to transfers under the General Data Protection Regulation[2] (GDPR).

The principle in the GDPR is that, in the event of a transfer, data must continue to benefit from protection substantially equivalent to that afforded by that text. Recital 101 of the GDPR states that "when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined". Chapter V of the GDPR contains specific provisions regarding data transfers.

In its so-called "Schrems II" ruling[3] the Court of Justice of the European Union (CJEU) emphasised the responsibility[4] of exporters and importers to ensure that the processing of personal data is carried out, and continues to be carried out, in compliance with the level of protection laid down in EU data protection legislation. According to the Court, exporters are also responsible for suspending the transfer, and/or terminating the contract if the importer is not, or is no longer, able to comply with its commitments on the protection of personal data. Thus, exporters relying on the transfer tools listed in Article 46 GDPR for their transfers of personal data have an obligation to assess the level of protection in third countries of destination and the need for supplementary measures. **Such an assessment is called "Transfer Impact Assessment" or 'TIA'.**

1.2 The objective of the TIA

A TIA must be carried out by the exporter subject to the GDPR, whether acting as controller or processor, with the assistance of the importer, before transferring the data to a third country outside the EEA where such transfer is based on an Article 46 GDPR tool. If the country of destination is covered by an adequacy decision of the European Commission, the exporter is not subject to this obligation. The exporter also does not need to carry out a TIA, if the transfer is carried out on the basis of one of the derogations listed in Article 49 GDPR.

---

[1] The European Economic Area (EEA) is made up of the Member States of the European Union, Norway, Iceland and Liechtenstein in which the GDPR has become applicable by incorporation into the EEA Agreement.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Judgment of the Court of Justice of the European Union of 16 July 2020, 'Schrems II', C-311/18, InfoCuria, https://curia.europa.eu/juris/document/document.jsf?mode=DOC&pageIndex=0&docid=228677&part=1&doclang=EN&text=&dir=&occ=first&cid=14906588

[4] According to the definition of the EDPB, an 'exporter' is a controller, joint controller or processor subject to the GDPR for processing, which discloses by transmission or otherwise makes personal data, subject to this processing, available to an 'importer', controller, joint controller or processor located in a third country (outside the European Economic Area (EEA)), whether or not it is subject to the GDPR for the processing in question in accordance with Article 3, or whether it is an international organisation. See Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (PDF, 807ko), EDPB, https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

The objective of a TIA is to **assess and document whether the importer will be able to comply with its obligations as set out in the transfer tool** chosen. To this end, the exporter must assess the level of protection offered by the local legislation and take into account the practices of the authorities in the third country in view of the intended transfer. Where necessary, the TIA should also assess whether supplementary measures would make it possible to remedy the shortcomings identified in data protection and ensure the level required by EU legislation.

1.3 The purpose of this guide

Following the Recommendations of the European Data Protection Board (EDPB) on measures that supplement transfer tools[5], the CNIL has developed this guide for exporters, to help them carry out their TIA.

This guide constitutes a methodology that identifies **the steps prior to carrying out a TIA and the different elements to be taken into account when carrying out a TIA**. It provides guidance on **how the analysis can be carried out** following the steps set out in the EDPB Recommendations and refers to the relevant documentation. It does not constitute an assessment of the laws and practices in third countries.

The use of this guide is not mandatory, other elements may also be taken into account and other methodologies applied.

As regards the steps prior to carrying out a TIA (Section 2), this guide is organised around the following criteria/requirements:

i. Existence of a transfer of personal data
ii. Need to carry out a TIA
iii. Responsibility to carry out the TIA
iv. Scope of the TIA, in particular taking into account onward transfers
v. Compliance with the principles of the GDPR

As regards the implementation of the TIA (section 3), this guide is organised according to the six different steps to be followed in order to carry out a TIA as recommended by the EDPB:

1. Know your transfer
2. Identify the transfer tool used
3. Evaluate the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool
4. Identify and adopt **supplementary** measures
5. Implement the **supplementary measures**
6. Reassess the level of protection at appropriate intervals and monitor potential developments that could affect it

[5] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (version 2.0), EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Step 1 enables the exporter to **describe the transfer**.

Step 2 consists of **documenting the tool that will be used to frame the described transfer** and the analysis concluding on whether or not to carry out a TIA.

Step 3 allows the exporter to **assess the legislation and practices in force in the country of destination** and to identify whether there are elements that could impinge the effectiveness of the safeguards provided through the transfer tool used (documented in step 2).

Step 4 consists of identifying **the existing security measures** (technical, contractual and organisational) that ensure an adequate level of data protection in the third country, taking into account the transfer (described in step 1) and the assessment of the third country's legislation and practices (step 3). If these measures are not satisfactory, the exporter **should identify the supplementary measures that need to be implemented** to ensure that the transferred data enjoy a level of protection in the third country that is substantially equivalent to that within the EEA.

Step 5 contains a model **action plan** for the operational implementation of the supplementary measures identified and possible procedural steps in Step 4.

Finally, **step 6** anticipates **future re-assessments** of the transfer by the exporter.

The description of the transfer (in step 1) and the identification of the transfer tool (in step 2) allow the characteristics and sensitivity of the transfer to be taken into account in the assessment of the legislation and practices of the third country and the effectiveness of the transfer tool (in step 3) to implement possible supplementary measures (in step 4).

2. Before carrying out a Transfer Impact Assessment

Before carrying out a TIA, several elements must be verified. It is recommended to document the analysis.

2.1 Existence of a transfer of personal data

Above all else, it is necessary to ensure that:

- **The data in question are personal data**

Article 4(1) of the GDPR defines personal data as *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.* [6]

- **A transfer of personal data is carried out**

In its Guidelines[7], the EDPB identified the following three cumulative criteria for determining whether a processing operation qualifies as a transfer:

1) A controller, joint controller or processor ('the exporter') is subject to the GDPR for the given processing

[6] See, for example, the various resources on the CNIL website:

- "Personal Data : definition", https://www.cnil.fr/en/personal-data-definition;
- "Sheet n°1: Identify personal data", https://www.cnil.fr/en/sheet-ndeg1-identify-personal-data

[7] See Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (PDF, 807 ko), EDPB, https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

2) The exporter discloses by transmission or otherwise makes the personal data in question available to another entity ('the importer'), whether it is a controller, joint controller or processor
3) The importer is based in a third country (non-EEA), whether or not the importer is subject to the GDPR for the given processing in accordance with Article 3, or the importer is an international organisation

As recalled by the EDPB[8], the concept of "transfer of personal data to a third country or to an international organisation" only applies to disclosures of personal data where two legally distinct entities (each of them a controller, joint controller or processor) are involved. Chapter V of the GDPR therefore does not apply to the transmission or making available of data within the same entity. This means that when an employee of a controller in the EU remotely accesses a database of their employer from a third country, for example during a business trip, this does not constitute a transfer within the meaning of the GDPR.

On the contrary, the transmission or making available of data between two separate entities belonging to the same group may constitute a transfer.[9]

Remote access from a third country to data stored in the EEA and cloud storage of data outside the EEA constitute a transfer where those activities are carried out by an entity legally different from that of the exporter.

2.2 Need to carry out a TIA

A TIA must be carried out before transferring the data to a third country where such transfer is based on a tool of Article 46 GDPR. For example, this concerns data transferred on the basis of European Commission Standard Contractual Clauses[10] or Binding Corporate Rules (BCRs).[11]

On the other hand, it is not necessary to carry out a TIA when:

- **The data is transferred to a country that has been recognised by the European Commission as offering an adequate level of protection**

Transfers of personal data to countries that have been recognised by the European Commission as offering an adequate level of protection[12] do not require the implementation of data transfer tools under Chapter V of the GDPR or supplementary measures. If the transfer of personal data takes place to such a country, this will ensure an adequate level of protection for the data in question. **In this case, there is no need to carry out a TIA.**

As the EDPB recalls in his Opinion 22/2024, for these adequate countries, the Commission has already taken into account: rules on onward transfers of data to another third country or an international organisation, case-law, as well as effective and enforceable rights of data subjects and effective administrative and judicial remedies for data subjects.[13]

Adequacy decisions may have a limited scope (e.g. Canada's Adequacy Decision only targets private sector organisations that process personal data in the course of commercial activities[14] and Japan's Adequacy Decision

---

[8] ibid., §20.

[9] ibid., §21.

[10] "Standard Contractual Clauses (SCC)", European Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[11] "Binding Corporate Rules (BCR)", European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[12] For the full list of countries that have been subject to such decisions, see "Adequacy decisions", European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[13] "Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)", EDPB, §92-93, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_en

[14] European Commission, Decision 2002/2/EC of 20 December 2001 establishing, pursuant to Directive 95/46/EC of the European Parliament and of the Council, the adequate level of protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002D0002

does not concern personal data transferred to broadcasting organisations, newspaper publishers, communication agencies or other media outlets, persons engaged in professional writing, universities, religious institutions and political bodies[15]) or may concern only certain entities certified in the third country (e.g. entities certified under the US Adequacy Decision[16]). Where the transfer of data does not fall within the scope of an adequacy decision, it is necessary to use one of the tools in Article 46 or to rely on a derogation in Article 49. In the former case, it is necessary to carry out a TIA.

Adequacy decisions are subject to periodic reviews. It is therefore recommended to regularly check the list of countries that have been subject to an adequacy decision in case new decisions have been taken or countries have been removed from the list.

- **The transfer is based on one of the derogations in Article 49**

A TIA will only be needed when one of the tools of Article 46 is used. Consequently, transfers based on one of the derogations in Article 49 may be carried out without any formality other than compliance with the conditions for their application laid down in that Article.

As the EDPB points out in its Guidelines 2/2018, "derogations as set out in Article 49 shall not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test"[17].

2.3 Qualification of the parties and responsibility for carrying out a TIA

The qualification (controller, joint controller or processor)[18] of the different entities involved in the transfer must be identified, as it determines the allocation of responsibilities and entails different obligations for the parties. The EDPB has produced Guidelines[19] dedicated to these concepts. Information is also available on the CNIL website.[20]

The TIA must be carried out by the exporter, whether acting as controller or processor, with the assistance of the importer. It is primarily the responsibility of the exporter to ensure that the data transferred in the third country is afforded an essentially equivalent level of protection and therefore to carry out the TIA. Nevertheless, the importer's assistance is essential for the implementation of the TIA as it has access to many necessary information for this assessment and has knowledge of the assessed legislation.

Several cases can be distinguished according to the role of the parties in the processing and their qualification:

[15] European Commission, Implementing Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data provided by Japan under the Personal Information Protection Act, Article 1, EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019D0419

[16] European Commission, Implementing Decision (EU) 2023/1795 of 10 July 2023 establishing, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the adequate level of protection of personal data provided by the EU-US data protection framework, EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023D1795. For the specific case of the United States, it is recommended to consult "Adéquation des États-Unis : les premières questions-réponses" [in French], CNIL, https://www.cnil.fr/en/adequation-des-etats-unis-les-premieres-questions-reponses

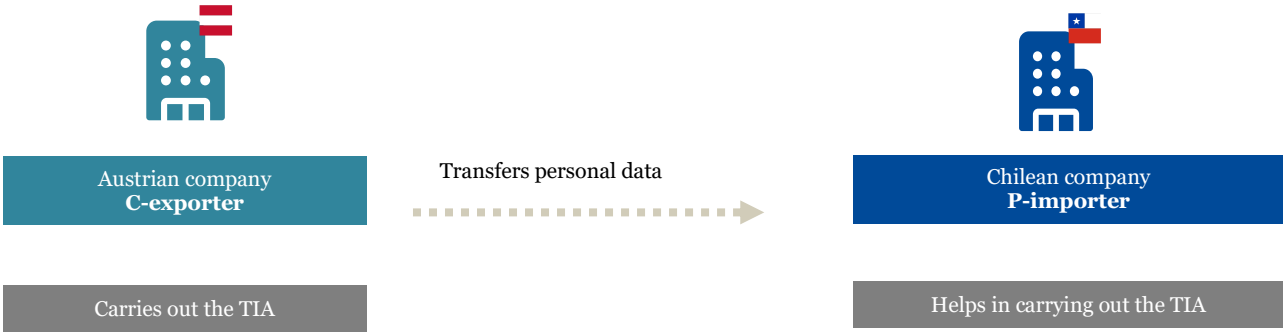
[17] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (PDF, 733 ko), p.4, EDPB, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

[18] Controller (or joint controller): the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; Processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (see Article 4(7) & (8) GDPR).

[19] See Guidelines 07/2020 on the concepts of controller and processor in the GDPR, EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[20] See for example "Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles" [in French], CNIL, https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees

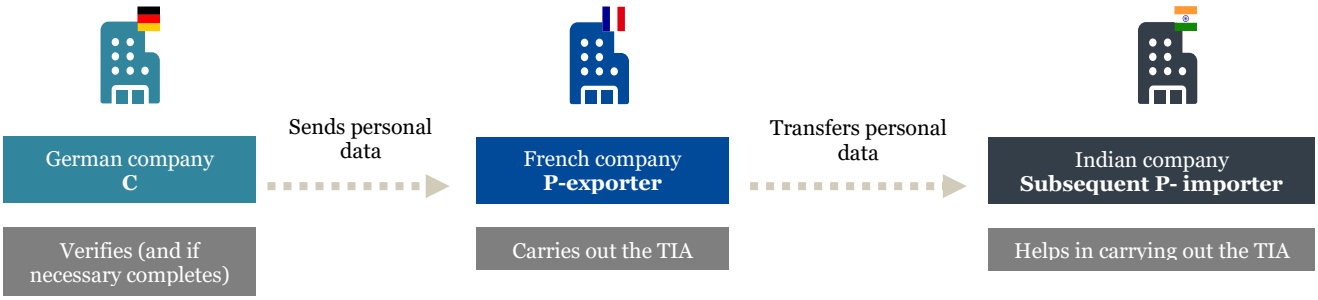
Case 1 - Controller in the EEA acting as an exporter transferring data to a processor acting as an importer in a third country:



The controller is required to carry out the TIA with the collaboration of the processor. In the context of a processing relationship, under Article 28(3)(h) GDPR, the processor is required to provide the controller with information to demonstrate compliance with his obligations.[21] This information may contain any relevant material enabling the controller to carry out the analysis of local legislation and practices, in particular with regard to access to data by public authorities.

Concrete evidence on the legislation and practices of the authorities may include, as appropriate, reports on access to data transferred from the EEA by the authorities of the third country, reports on access requests received in the past by the data importer or by its processor or by actors in the same sector of activity, information on the legislation of the third country with translations into the working language of the parties or information by the competent authorities on the handling of appeals where such appeals are exercised by nationals of EEA Member States.[22]

Case 2 - Processor subject to the GDPR acting as an exporter transferring data on behalf of a controller subject to the GDPR to a sub-processor acting as an importer in a third country:



In the event that the transfer of the data outside the EEA (in India in the diagram above) is carried out by the processor (the French company) and not the controller (the German company in the diagram), the processor is

[21] The EDPB states in its Guidelines 07/2020: 'The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR."*; "The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on [...] data location, transfers of data, who has access to data and who are the recipients of data, sub- processors used, etc."*

[22] It is possible to rely on any reliable source such as those cited in Annex 3 of EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, ("Possible sources of information to assess a third country" in §144), EDPB, https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf .

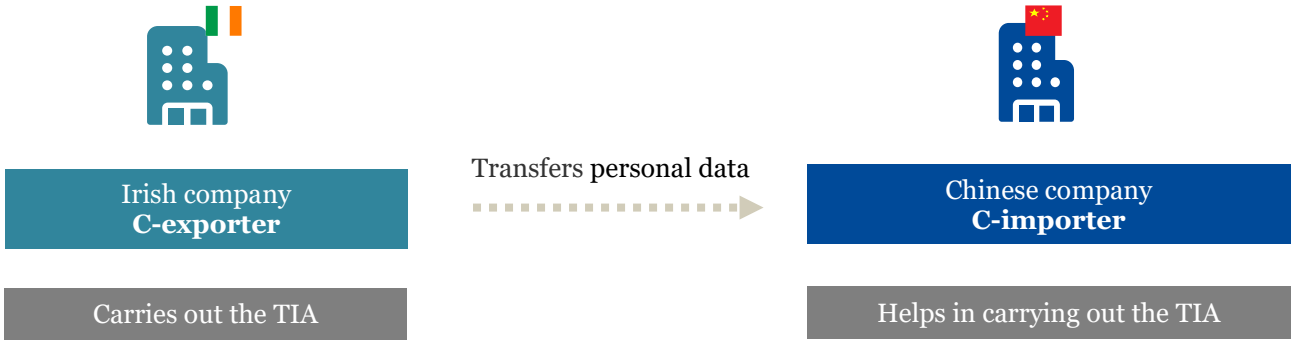
acting as an exporter, hence it is its responsibility to ensure the compliance of its transfer and to carry out the TIA.

Pursuant to Article 28(3)(h) GDPR, the processor (the French company) is required to provide the controller (the German company) with information to demonstrate compliance with the latter's obligations, including the TIA performed. It should be noted that the transmission by the exporting processor (the French company) of a simple conclusion or an executive summary of its TIA or its assessment on the legislation of the third country, without the provision of concrete evidence, does not enable it to fulfil its obligations.[23]

Furthermore, the final decision on whether or not to engage this processor and its sub-processor (the French and Indian companies) or to maintain the contractual relationship with them rests with the controller (the German company) who has the obligation to verify the safeguards offered under Article 28(1) GDPR. The higher the risk to the rights and freedoms of data subjects, the more important the checks carried out should be.[24] This can be done by relying on the information received from its Processor – including its TIA – and supplementing it if necessary (e.g. if it is incomplete, inaccurate or raises questions).

Case 3 - Controller subject to the GDPR acting as an exporter transferring data to a controller in a third country

In the context of a data transfer between a controller subject to the GDPR acting as an exporter and a controller based in a third country acting as an importer, it is the responsibility of the exporter to ensure that the data transferred in the third country enjoys a level of protection essentially equivalent to that guaranteed within the EEA and therefore to carry out the TIA with the help of the importer.



[23] The EDPB specifies in §96 of his Opinion 22/2024 : *"the controller should assess the appropriate safeguards put in place and be attentive about any problematic legislation that could prevent the sub-processor from complying with the obligations established in its contract with the initial processor. More specifically, the controller should ensure that such "a transfer impact assessment" is carried out, in line with the case-law, and as explained in EDPB Recommendations 01/2020. The documentation relating to the appropriate safeguards put in place, the "transfer impact assessment" and the possible supplementary measures should be produced by the processor/exporter (where appropriate in collaboration with the processor/importer). The controller can rely on the assessment prepared by the (sub-)processor and if necessary build on it. For example, where the assessment received by the controller seems incomplete, inaccurate or raises questions, the controller should ask for additional information, verify the information and complete/correct it if needed, keeping in mind that the assessment should be in line with EDPB Recommendations 01/2020 and the steps set out therein98. This includes identifying laws and practices* relevant in light of all circumstances of the transfer99 and identifying appropriate supplementary measures if necessary"

[24] See the executive summary and §60 of EDPB Opinion 22/2024: *Where transfers of personal data outside of the EEA take place between two (sub-)processors, in accordance with the controller's instructions, the controller is still subject to the duties stemming from Article 28(1) GDPR on 'sufficient guarantees', besides the ones under Article 44 to ensure that the level of protection guaranteed by the GDPR is not undermined by transfers of personal data. The processor/exporter should prepare the relevant documentation, in line with the case-law and as explained in EDPB Recommendations 01/2020. The controller should assess and be able to show to the competent SA such documentation. The controller may rely on the documentation or information received from the processor/exporter and if necessary build on it. The extent and nature of the controller's duty to assess this documentation may depend on the ground used for the transfer and whether the transfer constitutes an initial or onward transfer.*" The EDPB also states that "*SAs should assess whether the controller is able to demonstrate that the verification of the sufficiency of the guarantees provided by its (sub-)processors has taken place to the controller's satisfaction. The controller may choose to rely on the information received from its processor and build on it if needed (for example, where it seems incomplete, inaccurate or raises questions). More specifically, for processing presenting a high risk to the rights and freedoms of data subjects, the controller should increase its level of verification in terms of checking the information provided.*"

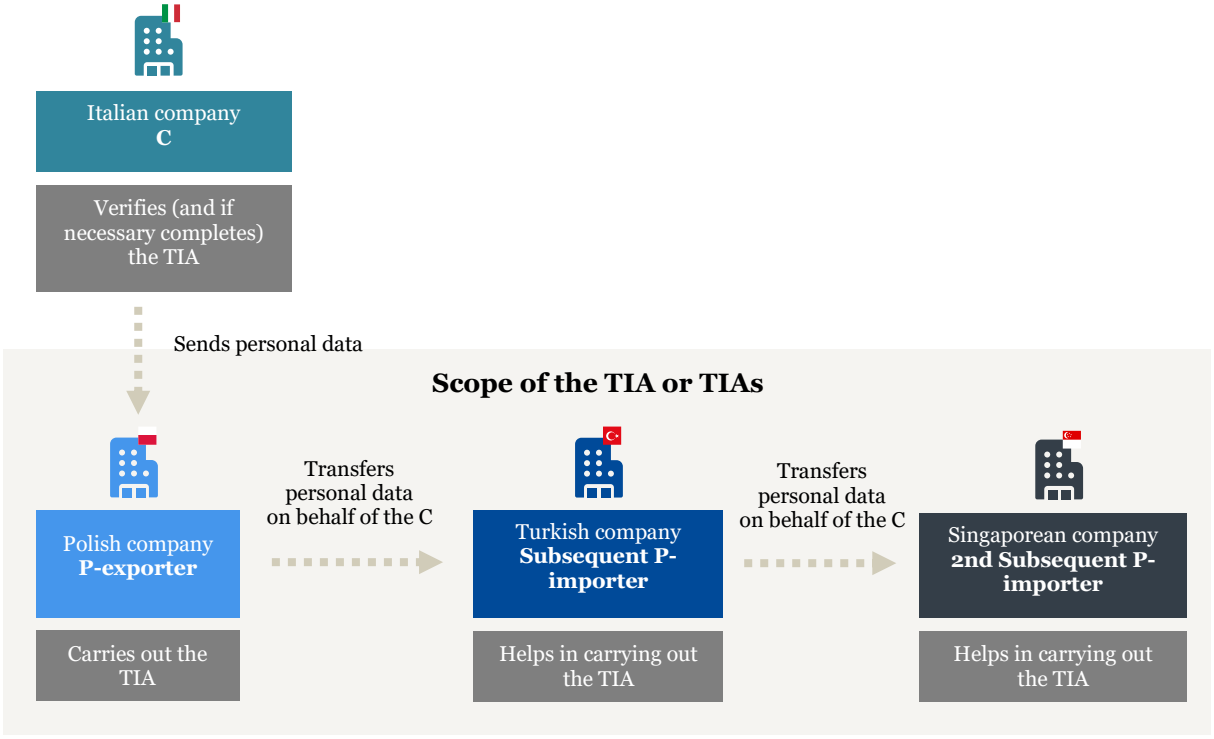
2.4 Scope of the TIA and consideration of onward transfers

The first step in carrying out the TIA is to map the data transfers (see step 1 of this guide). This mapping consists in properly identifying the importer and the third country. It allows the data exporter (and *ultimately the* controller, if the transfer is not carried out by itself) to identify the supplementary measures to be put in place (see steps 4 and 5).

The exporter must take into account in its analysis the entire data flow, including onward transfers, so that the controller (whether acting as the exporter or not) can assess the risks associated with all data transfers outside the EEA.[25]

A TIA may concern a single transfer or a set of transfers. Therefore, the exporter has the choice to document its analysis within the same or several documents. In the event of a change in the transfer chain, the exporter may modify the existing analysis or make a new analysis that it links to the pre-existing analyses it has already carried out. If the exporter is a processor, it must share this information with the controller.

Besides, any onward transfer is subject to compliance by the importer with the obligations set out in the transfer tool used. If Standard Contractual Clauses (SCCs)[26] have been concluded, the data importer undertakes not to disclose the personal data to a third party located outside the European Union to the same country as the data importer or to another non-adequate third country (hereinafter referred to as "onward transfer"), unless the third party is bound by the SCCs or agrees to be bound by them, under the appropriate module. Otherwise, an onward transfer by the data importer can only take place if the conditions laid down in the SCCs are met (Module 1, Article 8.7 and 8.8; modules 2 and 3 – Article 8.8) and provided that it complies with its obligations to keep the documentation necessary to demonstrate its conformity (modules 1 and 3, Article 8.9; Module 2 – Article 8.8).



[25] In paragraph 97 of its Opinion 22/2024, the EDPB states that "controllers should be able to show documentation relating to such onward transfers. This means that the controller should receive this information from the (sub-)processors/exporters, showing that the importers actually comply with the requirements for onward transfers as laid down in the appropriate safeguards instrument."

[26] See the Standard Contractual Clauses published by the European Commission, EUR-Lex, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

2.5 Compliance of the transfer with the principles of the GDPR

A transfer of data, like any other processing, must comply with all the principles of the GDPR. According to Article 5 GDPR, the controller must (directly if it is the exporter itself or through its processor if the latter is the exporter) ensure that the transfer is lawful and based on one of the legal bases of Article 6 and, where applicable, Article 9 GDPR. The data must also be adequate, relevant and limited to what is necessary for the purposes for which they are processed. It is therefore necessary to ensure that the data transferred are limited to what is strictly necessary for the purposes pursued by the transfer.

It is also necessary to ensure that data subjects are informed in accordance with Articles 13 and 14 GDPR. It is preferable, where possible, to disclose or transmit anonymised data in place of personal data, while ensuring that the anonymisation process is used effectively identification according to EDPB's Guidelines.[27] In this case, the GDPR does not apply.

3. The different steps of the TIA

To carry out a TIA, it is recommended to follow the following 6 steps:

3.1 Know your transfer (step 1)

In order to ensure a level of protection essentially equivalent to the data transferred, wherever it is processed, it is first necessary to describe the transfer. The description of the transfer (in step 1) allows its characteristics and sensitivity to be taken into account when assessing the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool (in step 3) with a view to putting in place possible supplementary measures (in step 4).

To complete the table below, it is possible to use pre-existing internal documentation, such as the record of processing activities or the contract governing the transfer.

It is also possible to ask this information to the data importer.

Exporter	
Name of the exporter	
Contact point and contact details (department or person responsible internally for the transfer)	

[27] For more details on anonymisation, see Article 29 Working Party (G29), Opinion 05/2014 on Anonymisation Techniques (PDF, 721 ko), European Commission, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf ; as well as "L'anonymisation de données personnelles" [available in French], 05/19/2020, CNIL, https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles .

Exporter	
Exportation country	
Exporter qualification in the context of data transfer[28]	☐ Controller ☐ Joint controller ☐ Processor *If 'Processor' or 'Joint controller', specify the name of the controller or other joint controllers:*
Any other useful information	

Importer	
Name of the importer	
Contact point and contact details (department or person responsible internally for the transfer)	
Importation country	
Importer qualification in the context of data transfer	☐ Data controller ☐ Joint controller ☐ Processor If *'Processor' or* ***'Joint controller',*** *specify the name of the controller:*
Nature of the importer's activities[29]	*Specify the nature:* *Is it a data importer specifically protected by the legislation of the country of destination of the data?* [30]

[28] See EDPB, Guidelines 07/2020, op.cit.

[29] Information facilitating the identification of the applicable legislation in the third country.

[30] A data importer in a third country may be specifically protected by national law, for example for the purpose of providing medical treatment to a patient, or legal services to a client. See §91, EDPB, Recommendations 01/2020 on measures supplementing transfer instruments to ensure compliance with the EU level of protection of personal data.

Importer	
Any other useful information	

Transfer	
Processing activities of the importer on the transferred data (e.g.*IT support, marketing, cloud software provision, data hosting)*	
Type of transfer (how *the data are made available to the importer*)	☐ **Remote access without the possibility to download/store** - The personal data is hosted by the exporter within the EEA. The importer does not have the possibility to download copies of the data, but can access them remotely from an inadequate non-EEA country. ☐ **Remote access with the possibility to download/store** - Personal data is hosted by the exporter within the EEA. The importer has the possibility to access the data from a third country and if necessary to download and store copies of the data in an inadequate EEA third country. ☐ **Transmission and hosting/local storage** - The importer hosts or stores the personal data in a non-adequatenon-EEA country. ☐ **Other**
Transfer method (e.g. *transmission by secure file transfer protocol (SFTP), transmission by email, connection via an application programming interface (API), connection to a remote server, storage of data in a physical medium and sending, etc.)*	
Format of data transferred	☐ In plain language ☐ Encrypted ☐ Pseudonymised ☐ Other *If 'Other', specify:*
Frequency of transfers	☐ Single transfer ☐ One-off/occasional transfer (*recurrence to be specified*): ☐ Regular transfer (*recurrence to be specified*):

Transfer	
Possibility of onward transfers for the importer (*see section 2.4 above*)	☐ Yes ☐ No *If **yes**, please specify:*
Categories of personal data transferred	☐ Identification data (*please specify*): ☐ Contact details (*please specify*): ☐ Data relating to family life (*please specify*): ☐ Data relating to working life (*please specify*): ☐ Service usage data (*please specify*): ☐ Other (*please specify*):
Special categories of personal data transferred ("sensitive data")	☐ Data revealing racial or ethnic origin (*please specify*): ☐ Data revealing political opinions (*please specify*): ☐ Data revealing religious or philosophical beliefs (*please specify*): ☐ Data revealing trade union membership (*please specify*): ☐ Genetic or biometric data for the purpose of uniquely identifying a natural person (*please specify*): ☐ Health data (*please specify*): ☐ Data concerning the sex life of a natural person (*please specify*): ☐ None of the above categories
Other highly personal data transferred	☐ Data on criminal convictions, offences[31] (*please specify*): ☐ National identification number[32] (*please specify*): ☐ Geolocation data[33] (*please specify*): ☐ Financial data likely to be used for fraudulent payments[34] (*please specify*): ☐ Other (*please specify*): ☐ None of the above categories

[31] Article 10 GDPR

[32] Article 87 GDPR

[33] See Article 29 Working Party (G29), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p.11, European Commission, https://ec.europa.eu/newsroom/article29/items/611236

[34] *Idem*.

Transfer	
Categories of data subjects	
Vulnerable persons among the data subjects (e.g. *minors, dependent persons)*	☐ Yes ☐ No If *'Yes'*, specify:
Total or partial nature of the transfer[35] (*if relevant*)	☐ Total ☐ Partial *If 'partial', specify the percentage (if possible):*
Volume of data transferred (*if possible*)	
Number of data subjects (*if possible*)	
Proposed start date of transfer (*if possible*)	
Envisaged end date or duration of the transfer (*if possible*)	

[35] The transferred data representing all or only part of the processed data.

3.2 Identify the transfer tool used (step 2)

The identification of the transfer tool used completes the description of the transfer (in step 1). It is necessary to assess its effectiveness (in step 3).

Transfer tool of Article 46 GDPR	
Article 46 transfer tool used to frame the transfer	☐ Standard Contractual Clauses (SCC)[36] (Module used to be specified): ☐ Binding Corporate Rules (BCR) "Controller"[37] ☐ Binding Corporate Rules (BCR) "Processor"[38] ☐ Code of conduct[39] ☐ Certification mechanism[40] ☐ Ad hoc contractual clauses
Evidence and documentation of the transfer tool in place (e.g. contract signed with the data importer, certificate of certification of the data importer, copy of the BCRs with the list of entities forming part of the BCRs including the data importer)	

If the transfer is based on one of the transfer tools of Article 46 GDPR, it is necessary to carry out a TIA and it is appropriate to proceed to step 3.

If it is not necessary to carry out a TIA (see section 2.2), it is recommended to document the decision not to carry out a TIA.

[36] See the Standard Contractual Clauses published by the European Commission. In its FAQ on SCCs, the European Commission states that an additional set of SCCs dedicated to transfers to importers subject to the GDPR is being developed. Once this new game is adopted, it will be possible to use it to frame transfers to importers subject to the GDPR. See §25 of FAQ. "New Standard Contractual Clauses - Questions and Answers overview", European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

[37] For BCR-Controller, see Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_en

[38] For BCR-Subcontractors, see G29 Recommendation on the approval of the Processor Binding Corporate Rules form (wp265), European Commission, https://ec.europa.eu/newsroom/article29/items/623848/en and Working Document on Binding Corporate Rules for Processors (wp257rev.01), European Commission, https://ec.europa.eu/newsroom/article29/items/614110/en

[39] See Guidelines 04/2021 on Codes of Conduct as tools for transfers, EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en

[40] See Guidelines 07/2022 on certification as a tool for transfers, EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en

3.3 Assess the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool (step 3)

Once a clear vision of the transfer and the tool used is obtained, the third step is to determine whether there are elements in the legislation or practices of the importing third country that could undermine the effectiveness of the guarantees of the tool used or prevent the exporter or importer from fulfilling their obligations. The description of the transfer (in step 1) allows its characteristics and sensitivity to be taken into account when assessing the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool (in step 3).

The assistance of the importer is essential for this exercise: it is up to the exporter to ask it to provide an analysis of its legislation, in particular as regards to access to data by the authorities, or at least to provide a list of the applicable laws. It is therefore important to involve the importer in the implementation of the TIA as the importer must follow the instructions of the exporter and the controller (if the exporter is a processor).

To complete this step, it is recommended to consult Annex 3 of the EDPB Recommendations on measures that supplement transfer tools, which lists, in a non-exhaustive manner, sources of information that can be used. These sources must be relevant, objective, reliable, verifiable and publicly available or otherwise accessible.

It is possible to rely on the CNIL's Data protection around the world page which contains information about the data protection framework in the third country (existence of a data protection law and a data protection authority).

For the analysis of data access legislation by public authorities, you can also rely on reports from international organisations and expert analyses such as analyses commissioned by the EDPB for certain countries. These analyses should be completed and updated as necessary.

It is recommended to share the analyses through networks of DPOs, professional federations as well as groups of companies or administrations.

Data protection legislation		
What is the data protection framework applicable to the importer?	*Reference of the text(s):*	
What is its scope?	☐ General framework ☐ Sectoral application	*If sectoral application, specify:*
Accession of the third country to international data protection treaties	☐ Yes ☐ No	*If yes, please specify:*
Is there a competent data protection authority (or administrative body with comparable powers) in the third country?	☐ Yes ☐ No	*Name of authority:*

Data protection legislation		
Is this authority/entity independent?[41]	☐ Yes ☐ No	*Justify:*
What are data subjects' rights?	**Data Subjects Rights**	
	Right of access ☐ Yes ☐ No	*If yes, reference:*
	Right of rectification ☐ Yes ☐ No	*If yes, reference:*
	Right of deletion ☐ Yes ☐ No	*If yes, reference:*
	Right to object to the processing for specific situations ☐ Yes ☐ No	*If yes, reference:*
	Right to object to automated decision-making ☐ Yes ☐ No	*If yes, reference:*
	Other rights ☐ Yes ☐ No	*If yes, please specify:*
	Are the legal restrictions on these rights necessary and proportionate in a democratic society?	*If yes, please specify:*

[41] In order to determine whether the authority is independent, it is possible to rely on Articles 52 to 54 of the GDPR, on Article 15 of Convention 108+ of the Council of Europe, https://www.coe.int/en/web/data-protection/convention108-and-protocol and on the work of the World Privacy Assembly (WPA):

- Article 5.1 of its Rules of Procedure (PDF, 224 ko), GPA, https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-Rules-and-Procedures-October-2020.pdf;
- Principle B.2 of its Accreditation Principles (PDF, 189 ko), GPA, http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Accreditation-Features-of-Data-Protection-Authorities.pdf; and
- the document of the Working Group on the future of the Conference "Interpretation of the criteria of autonomy and independence", GPA, https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence-criteria_post-Coe-comment.pdf.

It is also possible to build on the more general work of the Organisation for Economic Cooperation and Development (OECD):

- Being an Independent Regulator, https://www.oecd.org/en/publications/being-an-independent-regulator_9789264255401-en.html;
- The Governance of Regulators, https://www.oecd.org/en/publications/the-governance-of-regulators_24151440.html;
- Creating a Culture of Independence, https://www.oecd.org/en/publications/creating-a-culture-of-independence_9789264274198-en.html;

Data protection legislation		
	☐ Yes ☐ No	
Remedies and Sanctions	Are there effective legal remedies? ☐ Yes ☐ No	*Justify:*
	Are there effective and dissuasive sanctions? ☐ Yes ☐ No	*Justify:*
	Can these rights and remedies be exercised by data subjects in the EEA? ☐ Yes ☐ No	*Justify:*

Laws and/or practices allowing access to data		
Are there supervisory laws **applicable to the importer** laying down obligations to disclose the personal data transferred or to grant access to such data to public authorities?[42] ☐ Yes ☐ No	*If yes, list:*	
	References	*Description (scope, public authority concerned, nature of obligation, etc.)*
Are there any practices **applicable to the importer** entailing obligations to disclose the personal data transferred or to grant access to such data to public authorities?[43] ☐ Yes ☐ No		

[42] These laws may be of general application, concern the application of criminal law or the protection of national security. They may involve authorities such as government agencies, regulators, tax authorities, police, intelligence agencies, etc.

[43] *Idem.*

Essential guarantees[44]	
Is access to data as identified above governed by clear, precise and accessible rules? ☐ Yes ☐ No	*Justify:*
Is access to data necessary and proportionate in a democratic society to safeguard one of the purposes listed in Article 23(1) GDPR?[45] ☐ Yes ☐ No	*Justify:*
Is access to data controlled by an independent monitoring mechanism? ☐ Yes ☐ No	*Justify:*
Is the public authority concerned subject to transparency and regular monitoring obligations? ☐ Yes ☐ No	*Justify:*
Does the data subject have general (non-nationality) and effective remedies before an independent and impartial body? ☐ Yes ☐ No	*Justify:*

[44] See EDPB Recommendations 02/2020 on European essential safeguards for supervisory measures.

[45] These objectives are: (a) national security; (b) national defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including in the monetary, budgetary and fiscal fields, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, detection, investigation and prosecution of breaches of the ethics of regulated professions; (h) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority, in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the execution of civil law claims.

Rule of law		
Are there any rule of law issues affecting the ability of data subjects affected by the transferred data to seek redress against unlawful access to personal data? ☐ Yes ☐ No	*If yes, list:*	
	Issue	*How it affects the exercise of rights for data subjects*

Requests received	
Can the importer demonstrate that he has not received a request for access or has been the subject of direct access by the authorities of the third country to personal data of EEA nationals (at least in recent years)? ☐ Yes ☐ No	*If **yes**, specify here how it can demonstrate this:*[46] *If **not**, specify here the type of applications received, the quantity and manner in which they have been processed and/or the reasons why he thinks he may be the subject of them in the future:*
Can it be demonstrated that there is no reason to believe that the importer will be the subject of a request for access or direct access by the authorities of the third country, in particular because the legislation or issues identified will not in practice apply to the data transferred and to the importer (taking into account its sector of activity and the history of requests for access by the authorities of the third country)?[47] ☐ Yes ☐ No In this case, it is possible to decide to proceed with the transfer without implementing supplementary measures.	*If **yes**, specify here how it can demonstrate this:*[48]

Conclusion
☐ The transfer tool is effective in light of the assessment of local legislation and practices and it is possible to carry out the transfer without supplementary measures (1). ☐ The transfer tool is not effective in the light of the assessment of local legislation and practices and supplementary measures need to be put in place (2).

[46] For example, through its transparency report on requests for access by authorities to the data of the exporter or other exporters.

[47] In some cases where the transfer tool is not effective in the light of the assessment carried out but there is no reason to believe that the problematic legislation will be applied in practice to the transferred data and/or to the importer, it is possible to decide to still proceed with the transfer without implementing additional measures. It is then necessary to demonstrate and document this assessment where appropriate in collaboration with the importer, also taking into account the experience of other actors operating in the same sector and/or in sectors related to similar transferred personal data and other sources of information. See EDPB, Guidelines 01/2020, §43.3

[48] For example, through material published by other actors operating in the same and/or related sectors.

☐ The transfer tool is not effective in the light of the evaluation carried out but there is no reason to believe that the problematic legislation will be applied in practice and it is decided to proceed with the transfer without implementing supplementary measures (3).

Justify:

If the conclusion is that the transfer tool **is effective** in the light of the assessment carried out (1) or that despite the ineffectiveness of the tool, it is possible to carry out the transfer without putting in place supplementary measures (3), proceed to Step 6.

If the conclusion is that the transfer tool is not effective in light of the assessment carried out (2), proceed to step 4 in order to identify supplementary measures.

3.4 Identify and adopt supplementary measures (Step 4)

It is necessary to identify on a case-by-case basis what supplementary measures could be effective for the transfer to a given third country. The description of the transfer in step 1 allows, in particular, its characteristics and sensitivity to be taken into account for the assessment of the supplementary measures to be put in place. The higher the risk to the rights and freedoms of data subjects, the greater the checks carried out and the supplementary measures to be implemented.[49]

These measures are referred to as 'supplementary' because they supplement the transfer tool used to ensure compliance with the level of protection of personal data in the EEA. It is therefore necessary to identify in the table below both measures already implemented, if any, as well as newly identified measures.

Annex 2 of the EDPB Recommendations on measures that supplement transfer tools provides a non-exhaustive list of technical, contractual and organisational measures that can be implemented as use cases. It also presents use cases for which the EDPB is unable to identify effective measures.[50]

It may be necessary to combine several supplementary measures. In most cases, contractual and organisational measures are not sufficient to prevent possible access to the data by the authorities of the third country and need to be complemented by properly implemented technical measures.[51]

The effectiveness of the supplementary measures may vary depending on the transfer described in Step 1 and on the third country, hence the importance of conducting a detailed analysis in Step 3. **In some cases, the conclusion will be that there are no supplementary measures to ensure a level of protection essentially equivalent to European law for the transfer in question, which should lead to a waiver of the transfer of the data in question.**

This process of identifying supplementary measures should be undertaken with due diligence, in collaboration with the importer and should be documented. The involvement of the Chief Information Systems Officer is essential. It is recommended that the opinions or analyses of the persons or entities consulted (e.g. DPO, legal and technical advice, information systems officer, data protection authority) be annexed to the TIA.

---

[49] In its Opinion 22/2024, the EDPB states that "for processing presenting a high risk to the rights and freedoms of data subjects, the controller should increase its level of verification in terms of checking the information provided." With regard to transfers specifically, it further states: "the controller's obligation to verify whether the (sub-)processors present 'sufficient guarantees' to implement the appropriate measures determined by the controller should apply regardless of the risk to the rights and freedoms of data subjects. However, the extent of such verification will in practice vary depending on the nature of these technical and organisational measures, which may be stricter or more extensive depending on the level of such risk". See EDPB, Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), Executive Summary, §§60 and 83.

[50] See EDPB Recommendations 01/2020, Use Cases 6 and 7, §§93-97.

[51] See EDPB, Recommendations 01/2020, §53: "*Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices. Indeed there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purpose.*"

Supplementary measures already implemented			
Description (For each measure, provide a description, whether it is implemented by the importer or exporter and to what extent it complies with the EDPB Recommendations)			**Impact of measures** (For each measure, specify which risk(s) is/are mitigated)
Technical measures *(for the technical measures to be effective verify all the control points mentioned in the footnotes)*	☐ Pseudonymisation[52] ☐ Encryption[53] ☐ Other (please specify):		

[52] See EDPB, Recommendations 01/2020, use case 2, §85:

> *1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information,*
>
> *2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA,*
>
> *3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional*
>
> *information, and*
>
> *4. the controller has established by means of a thorough analysis of the data in question – taking into account any information that the public authorities of the recipient country may be expected to possess and use - that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information*

[53] See EDPB, Recommendations 01/2020, use case 3, §90:

> *1. a data exporter transfers personal data to a data importer in a jurisdiction where the law and/or practice allow the public authorities to access data while they are being transported via the internet to this third country without the European essential guarantees concerning these access, transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of this third country,*
>
> *2. the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure,*
>
> *3. specific protective and state-of-the-art measures are used against active and passive attacks on the sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors, 4. in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,*
>
> *5. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities when data is transiting to this third country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them (see footnote 80 above),*
>
> *6. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,*
>
> *7. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification, 8. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection.*

Supplementary measures already implemented			
Organisational measures[54]	☐ Access requests documentation (requests received, reply, legal reasoning, actors involved) ☐ Data minimization (strict and granular access, privacy policies, access based on the need-to-know principle, control through audits, disciplinary measures) ☐ Governance (information and involvement of the data protection officer or GDPR referent for all access requests) ☐ Adoption of security and data protection standards (certification and compliance with safety standards) ☐ Internal policies and procedures for processing access requests ☐ Allocation of responsibilities between entities in the same group, appointment of specific teams to handle access requests, training of staff responsible for managing such requests ☐ Other (please specify):		
Contractual measures[55]	☐ Inclusion of supplementary technical or organisational measures in a binding contract ☐ Transparency requirements ☐ Obligation of the importer to list laws, practices, measures to prevent access, requests for access, and to indicate whether he is legally prohibited from providing the above information ☐ Prohibition of the use of backdoors or processes that facilitate access to data ☐ Possibility to carry out an audit to verify compliance ☐ Notification of the exporter (and data subjects) in case of		

[54] See EDPB, Recommendations 01/2020, Section 2.3 Organisational measures, §§ 128-143:

[55] See EDPB, Recommendations 01/2020, Section 2.2 Additional contractual measures, §§98-127.

Supplementary measures already implemented			
	access to data by public authorities ☐ Commitment to challenge access requests ☐ Undertaking by the importer to review the legality of any disclosure order and challenge it if there are reasons to do so ☐ Commitment to seek interim measures to suspend the effects of the order until the court decides on the merits ☐ Commitment to inform in case of inability to comply with contractual commitments ☐ Sanctions for violations, including compensation of data subjects ☐ Termination of the contract in the event of failure to comply with obligations relating to data transfers ☐ Undertaking by the importer to provide the authorities of the third country with only the minimum information when responding to a request for access ☐ Undertaking of the importer to inform the authority of the third country of the incompatibility with data protection laws and simultaneously notify the exporter ☐ Data in clear can only be accessed with the explicit or implicit consent of the exporter ☐ Other (please specify):		
Conclusion		☐ The transfer tool, combined with these existing measures, **is effective** in the light of the assessment carried out. ☐ The transfer tool, combined with these existing measures, **is not effective** in the light of the assessment carried out. In such cases, it is necessary to consider further supplementary measures.	

New supplementary measures		
Description (For each measure, provide a description, whether it is implemented by the importer or exporter and to what extent it complies with the EDPB Recommendations)		**Impact of measures** (specify which risk(s) is/are mitigated by supplementary measures)
Technical measures (see examples above)		
Organisational measures (see examples above)		
Contractual measures (see examples above)		
Conclusion	☐ The transfer tool, combined with existing and new supplementary measures, **is effective** in the light of the assessment carried out. ☐ The transfer tool, combined with existing and new supplementary measures, **is not effective** in the light of the assessment carried out.	

If the conclusion is that the transfer tool, combined with these measures, is effective in the light of the assessment carried out, it is possible to transfer subject to the effective implementation of supplementary measures. In case already existing measures are sufficient, it is possible to go directly to step 6. In case supplementary measures are needed (in addition to already existing ones), it is recommended to go to step 5.

Following the completion of the TIA or during a re-assessment, if the conclusion is that it is not possible to put in place the necessary measures to ensure the effectiveness of the transfer tool, the planned transfer should not be implemented. If the transfer is already ongoing, it needs to be terminated. In the latter case, the importer will have to erase all data and prove them to the exporter, or return all data and erase existing copies.

3.5 Implement the supplementary measures (step 5)

Once the supplementary measures to ensure that the transferred data enjoy an essentially equivalent level of protection have been identified, it is recommended to list in the table below the actions to be taken to implement the new supplementary measures along with any procedural steps to be followed. This makes it possible to ensure that they are effective and to anticipate any obstacles (e.g. financial difficulties, unavailability of the competent teams, etc.).

The procedural steps to be followed may vary depending on the transfer tool on which the transfer is based. The EDPB Recommendations on measures that supplement transfer tools list some of these steps.[56]

[56] See EDPB Recommendations 01/2020,Section 2.5 Step 5, §§59-68. For example, the need for the exporter to apply to the competent authority for an authorisation where the SCCs have been amended and this restricts the rights and obligations contained therein or where the additional measures contradict the SCCs.

Action Plan	
Action 1 *Name:*	*Description:*
	Estimated cost in person/days (optional):
	Person(s) in charge (e.g. legal expert, technical expert, business department):
	Estimated date of completion:
Action 2 *Name:*	*Description:*
	Estimated cost in person/days (optional):
	Person(s) in charge (e.g. legal expert, technical expert, business department):
	Estimated date of completion:
…	…

Opinions
Opinion of the person in charge of data protection (or the Data Protection Officer, if applicable)
Opinion of the person in charge of security of the information system (or of the Chief Information Security Officer, if applicable)

Validation by the person responsible for the transfer according to internal governance rules

3.6 Re-evaluate at appropriate intervals (step 6)

It is recommended to reassess at appropriate intervals the transfer tool and, where appropriate, the supplementary measures that have been implemented for the transfer. This is essential to ensure that the transfer will be suspended or terminated if the transfer tool or supplementary measures are no longer effective in the third country. To this end, a periodic review of the transfer is recommended in the table below.

These appropriate intervals are to be determined on a case-by-case basis according to the country of destination of the data and the level of risk to the rights and freedoms of the data subjects involved in the transfer. In various circumstances, it may be necessary to reassess the transfer protection before the initial date of the next review, for example in the event of a change in the third country's law or practice, an importer's inability to comply with its commitments or a change in the European Commission's assessment of the law applicable in the third country. To this end, it is recommended to follow the legislative news in that country, in order to be able to anticipate whether the reassessment of data protection in that country is necessary.

Reevaluate Protection	
Interval between reviews (e.g. every 2 years)	
Date of next review	
Early review, if any, and justification for anticipation	