PRACTICAL GUIDE

IMPACT ANALYSIS DATA TRANSFERS

Final version

January 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table of contents

1. Introduction

1.1 Context

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

The principle instituted by the RGPD is that, in the event of transfer, data must continue to benefit from protection substantially equivalent to that offered by this text. Indeed, Recital 101 of the RGPD stresses that "it is important that, where personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organizations, the level of protection of natural persons guaranteed in the Union by this Regulation is not compromised". Chapter V of the RGPD includes specific provisions concerning data transfers.

In its so-called "Schrems II" ruling[3] , the Court of Justice of the European Union (CJEU) underlined the responsibility of exporters and importers[4] to ensure that the processing of personal data is carried out, and continues to be carried out, in compliance with the level of protection set by European Union 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 personal data protection commitments. Thus, exporters relying on the transfer tools listed Article 46 of the RGPD for their personal data transfers are obliged to assess the level of protection in third destination countries and the need to implement additional measures. **Such an assessment is known as a "*Analyse d'impact des transferts de données*" or "AITDin French.**

1.2 The AITD objective

A **DTIA must be carried out by the exporter subject to the RGPD, whether controller or processor, with the assistance of the importer, before transferring data to a third country outside the EEA when this transfer relies on an Article 46 RGPD tool**. If the destination country is covered by a European Commission adequacy decision, the exporter is not subject to this obligation. Nor does the exporter have to

---

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

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals 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 July 16, 2020, "Schrems II", C-311/18: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=3086778

[4] According to the EDPS definition, an "**exporter**" is a controller, joint or sub-processor subject to the RGPD for a processing operation, who communicates by transmission or makes accessible by another means the personal data in question to an "**importer**", controller, joint controller or processor who is located in a third country (outside the European Economic Area (EEA)), whether or not subject to the RGPD for the processing en cause in accordance with to article 3, or whether a international organization. See EDPS, Guidelines 05/2021 on the interaction between the application Article 3 and the provisions on international transfers of Chapter V of the RGPD: https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05- 2021_interplay_between_the_application_en.pdf

if the transfer is made on basis of one of the derogations listed article 49.
of the RGPD.

The aim a DTIA is to **assess** and document **whether the importer will be able to meet its obligations under the chosen tool in** the light of the legislation and practices of the third country of destination - in particular as regards potential access to personal data by authorities in the third country. To this end, the exporter must assess the level of protection offered by local legislation and take into account the practices of the authorities in the third country in view of the planned transfer. Where necessary, the DTIA must also make it possible to assess whether additional measures would make it possible to fill any gaps in data protection and ensure the level of protection required by EU legislation.

1.3 The purpose of this guide

Following on from the recommendations of the European Data Protection Committee (EDPS) on additional measures to complement transfer tools[5] , CNIL has drawn up this guide for exporters, to help them carry out their DTIA.

This guide is a methodology that identifies the steps prior to carrying out a DTIA and the various elements to be taken into account when performing a DTIA. It gives indications on how the analysis can be carried out, following the steps set out in the EDPS recommendations, and refers to relevant documentation. It does not constitute an assessment of third-country legislation and practices.

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

In terms of the steps to be taken prior to producing a DTIA (section 2), this guide is organized around the following points
of the following questions:

i. Existence a transfer of personal data
ii. Need to perform an AITD
iii. Responsibility for AITD
iv. AITD perimeter, including consideration of subsequent transfers
v. Compliance with RGPD principles

In terms of carrying out AITD (section 3), this guide is organized according to six different stages
to be followed when conducting a TDIA, as recommended by the EDPS:

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

[5] Recommendations 01/2020 on measures to complement transfer instruments to ensure compliance with the level of protection protection of data à personal personal from EU (version 2.0) (PDF, 658 kb), EDPS: https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

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

Step 2 involves **documenting the tool that will be used to frame the transfer** described and the analysis concluding whether or not a TDIA is necessary.

Step 3 enables the exporter to **assess the legislation and practices in force in the country of destination of** the data, and to identify if there are any elements that could the effectiveness of the guarantees provided by the transfer tool used (documented in step 2).

Step 4 consists in **identifying the** existing **security measures** (technical, contractual and organizational) ensure a sufficient level of data protection in the third country, taking into account the transfer (described step 1) and the assessment of the third country's legislation and practices (step 3). If these measures are not satisfactory, the exporter **identifies the additional measures that need to be implemented** to ensure that the data transferred enjoys a level of protection in the third country that is essentially equivalent to that within the EEA.

Step 5 contains a model **action** for the operational implementation of the measures.
and any procedural steps in step 4.

Finally, **step 6** anticipates **future revaluations** of the transfer by the exporter.

The description of the transfer (in step 1) and the identification of the transfer tool (in step 2) enable the characteristics and sensitivity of the transfer 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 (step 3), with a view to implementing any additional measures (step 4).

2. Before carrying out an impact analysis of DATA TRANSFERS

Before carrying out an AITD, several points need to be checked. We recommend documenting analysis.

2.1 Existence a transfer of personal data

Before doing anything else, you need to make sure that :

- **The data in question is personal data.**

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

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

In its guidelines[7] , the EDPS has identified the following three cumulative criteria to establish whether a treatment can be qualified as a transfer:

1) A , joint controller or processor ("exporter") is subject to the GDPR for the processing in question;

[6] See, for example, the various resources on the CNIL website:
- "Personal data: https://www.cnil.fr/fr/definition/donnee-personnelle
- "Identify personal data: https://www.cnil.fr/fr/identifier-les-donnees-personnelles

[7] See EDPS guidelines 05/2021 on the interaction between the application of Article 3 and the provisions on international transfers in Chapter V of the GDPR, EDPS: https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_en.pdf

2) The exporter discloses by transmission or otherwise makes available the personal data in question to another entity ("the importer"), whether it is a controller, joint controller or processor;

3) The importer is in a third country (outside the EEA), whether or not it is subject to the GDPR for the processing in question in accordance with Article 3, or is an international organization.

As the EDPS[8] points out, the notion of "transfer of personal data to a third country or to an international organization" only applies to the disclosure of personal data involving two legally distinct entities (each of which is a controller, a joint controller or a processor). Chapter V of the GDPR therefore does not apply to the transmission or provision of data within the same entity. This means that when an employee of a controller in the EU remotely accesses his employer's database from a third country, during a business trip for example, this does not constitute a transfer within the meaning of the RGPD.

On the other hand, the transmission or provision of data between two distinct 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 when these activities are carried out by an entity that is legally different from that of the exporter.

2.2 Need to perform an AITD

A DTIA must be carried out before transferring data to a third country when this transfer based on an Article 46 RGPD tool. For example, this concerns data transferred on the basis of European Commission standard contractual clauses[10] or *Binding* Corporate Rules *(BCR)*[11].

On the other hand, it is not necessary to perform an AITD when :

➢ The transfer is to a country that has been recognized by the European Commission as offering an adequate level of protection

Transfers of personal data to countries that have been recognized by the European Commission as offering an adequate level of protection[12] do not require the implementation of Chapter V data transfer tools of the GDPR or additional measures. If personal data is transferred to such a country, an adequate level of protection for the data in question is ensured. **In this case, it is not necessary to carry out a DTIA**.

As the EDPS points out in his opinion 22/2024, for these suitable countries, the Commission has already taken into account: rules on subsequent data transfers to another third country or an international organization, case law, as well as the effective and enforceable rights of data subjects and effective administrative and judicial remedies for data subjects[13].

---

[8] *ibid*, .§20
[9] *ibid*, §21.
[10] "Transfert de données: les clauses contractuelles types (CCT) de la Commission européenne", February 8, 2016, CNIL: https://www.cnil.fr/fr/transfert-de-donnees-les-clauses-contractuelles-types-cct-de-la-commission-europeenne
[11] "Les règles d'entreprise contraignantes (BCR)", CNIL: https://www.cnil.fr/fr/les-outils-de-la-conformite/les-regles-dentreprise-contraignantes-bcr
[12] For a full list of countries where such decisions have been taken, 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)*, §92-93, [in English] (PDF, 653 kb), EDPS: https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub- processors_en.pdf

Adequacy decisions may have a limited scope (for example, Canada's adequacy decision covers only private sector organizations that process personal data in the course of commercial activities[14] and Japan's adequacy decision does not concern personal data transferred to broadcasting organizations, newspaper publishers, communications agencies or other media organizations, persons engaged in professional editorial activities, universities, religious institutions and political bodies15) or concern only certain entities certified in the country concerned (for example, entities certified under the US adequacy decision[16]). When the data transfer does not fall within the scope of an adequacy decision, it is necessary to resort one of the tools Article 46 or to rely on a derogation Article 49. In the first case, an AITD is required.

Adequacy decisions are subject to periodic review. It is therefore advisable to regularly check the list of countries that have been the subject of a suitability decision, in case new decisions have been adopted or countries have been removed from the list.

- **The transfer is based on one of the derogations article 49.**

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

As the EDPS points out in his recommendations on additional measures/on derogations, "it is only in certain cases that the exporter may invoke one of the derogations provided for Article 49 of the GDPR, as long as he meets the required conditions. Derogations cannot become "the rule" in practice, but must be limited to specific situations "[17].

2.3 Qualification of parties and responsibility for carrying out a DTIA

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 EDPS has produced guidelines[19] dedicated to these concepts. Elements are also available on the CNIL[20] website.

The DTIA must be carried out by the exporter, whether acting as controller or sub-contractor, with the assistance of the importer. , it is primarily the exporter's responsibility to ensure that the data transferred to the third country benefits a level of protection essentially equivalent to that guaranteed within the EEA, and therefore to carry out the DTIA. Nevertheless, the importer has a great deal of information at his disposal for this assessment, and in particular,

---

[14] European Commission, Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002D0002

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

[16] European Commission, Implementing Decision (EU) 2023/1795 of July 10, 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data provided by the EU-US Data Protection Framework, EUR-Lex: https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=CELEX%3A32023D1795.
For the specific case of the United States, we recommend consulting the dedicated page "United States Adequacy: CNIL's first questions and answers", CNIL: https://www.cnil.fr/fr/adequation-des-etats-unis-les-premieres-questions-reponses.

[17] EDPS, Guidelines 2/2018 on derogations Article 49 of Regulation (EU) 2016/679, p.4

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

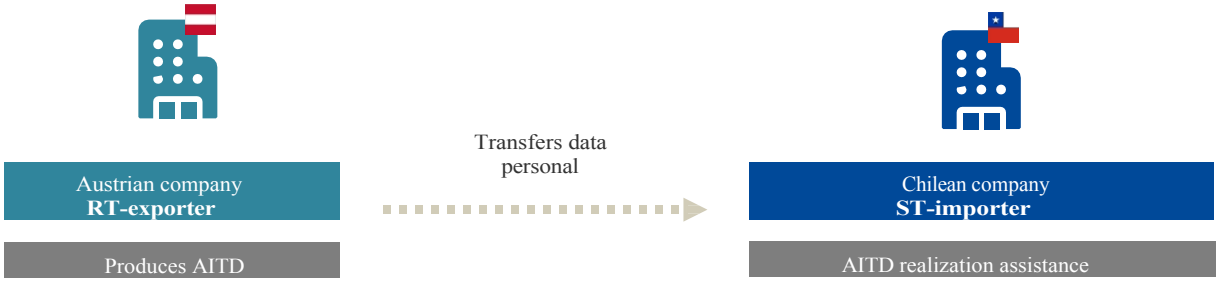
[19] See *Guidelines 07/2020 concerning the concepts of controller and processor in the RGPD* (PDF, 1, 58 MB), EDPS : https://www.edpb.europa.eu/system/files_en?file=2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

[20] See, for example, "Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles," July 8, 2020, CNIL, : https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees.

knowledge of the legislation of the country in which it is located, its cooperation is essential to the realization of the AITD.

Several cases can be distinguished depending on the role of the parties in the treatment and their qualification:

Case 1 - Data controller in the EEA acting transferring exporter data to a subcontractor acting as importer in a third country :



The controller is required to carry out the DTIA with the collaboration of the processor. , in the context of a subcontracting relationship, under Article 28(3)(h) of the GDPR, the processor is required to transmit to the controller information enabling it to demonstrate compliance with its obligations[21]. This information may contain any useful information enabling the data controller to carry out an analysis of local legislation and practices, in particular those of public authorities with regard to access.

Concrete information 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 its processor, or by players in the same sector of activity, information on the legislation of the third country, with translations into the working language of the parties involved, or information from the competent authorities on the handling of appeals when such appeals are lodged by nationals of EEA member states[22].

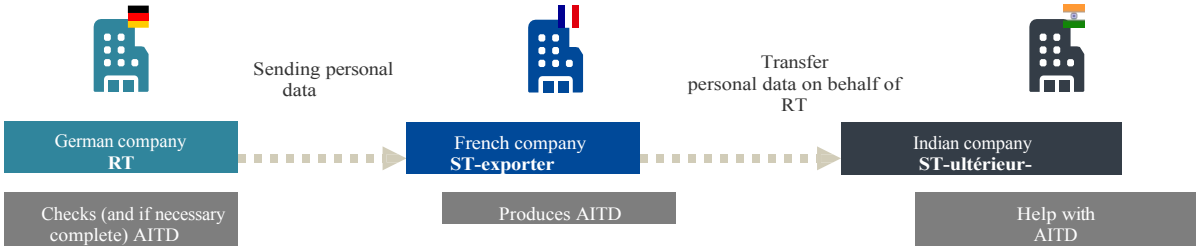
Case 2 - Subcontractor subject to the GDPR acting as an exporter transferring, on behalf a RT subject to the GDPR, data to a subsequent subcontractor acting as an importer in a third country:

In cases where the transfer of data outside the EEA (to India in the diagram below) is not carried out by the data controller (the German company in the diagram), but by its sub-processor (the French company), the latter thus acting exporter, it is its responsibility to ensure the compliance of its transfer and to carry out the DTIA.

---

[21] In its guidelines 07/2020, the EDPS states: "*[T]he [outsourcing] contract must specify the frequency and manner in which the flow of information between the processor and the controller should place, so that the latter is fully informed of the details of the processing that are relevant for demonstrating compliance with the obligations set out Article 28 of the GDPR; [t]his information should include data on [...] the location of the data, data transfers, persons who have access to the data and recipients of the data, subsequent processors used, etc.* ". https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and- processor-gdpr_en

[22] is possible to rely on any reliable source such as those cited in Appendix 3 of Recommendations 01/2020 on measures to complement transfer designed to ensure compliance with the EDPS's EU level of personal data protection ("Possible sources information for purposes of assessing a third country" in §144): https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures- supplement-transfer_en



Under Article 28(3)(h) of the GDPR, the processor (the French company) is required to transmit to the controller (the German company) the information to demonstrate compliance with the 's obligations, including the DTIA carried out. It should be noted that the transmission by the exporting processor (the French company) of a mere conclusion or executive summary of its DTIA or assessment on the legislation of the third country, without the provision concrete elements, does not enable it to meet its obligations[23].

Furthermore, the final decision on whether or not to engage this processor and its subsequent processor (the French and Indian companies) or to maintain the contractual relationship with them rests with the controller (the German company), which is obliged to verify the guarantees offered under Article 28(1) of the GDPR. The greater the risk to the rights and freedoms of data subjects posed by the processing, the greater the checks carried out should be[24]. To do so, it can rely on the information received from its processor - including its AITD - and supplement it if necessary (for example, if it is incomplete, inaccurate or raises questions).

Case 3 - Data controller subject to the RGPD acting as exporter transferring data to a data controller in a third country

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

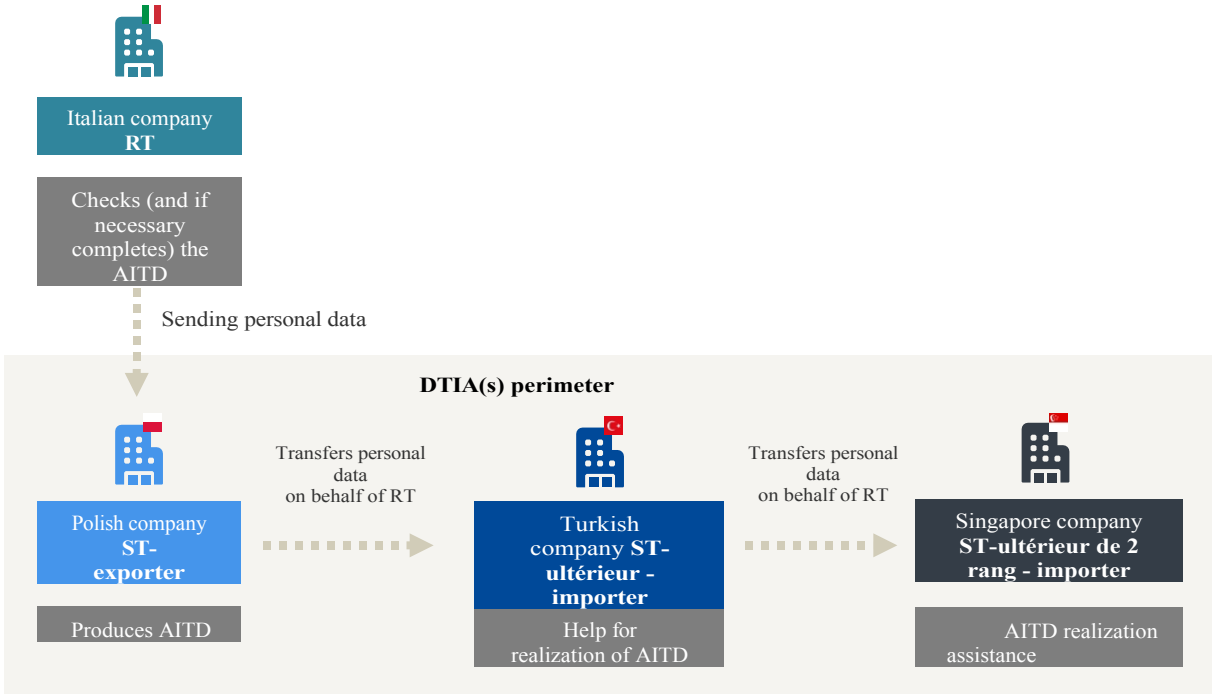
---

[23] The EDPS states in §96 of its opinion 22/2024, *op.cit*. (translated into French by CNIL): "The controller must assess the appropriate safeguards in place and be alert to any problematic legislation that could prevent the sub-processor from complying with the obligations set out in its contract with the original processor. More specifically, the controller must ensure that a "transfer impact " is carried out, in line with case law and as explained in EDPS recommendations 01/2020. Documentation relating to the appropriate safeguards put in place, the "transfer impact analysis" and any additional measures must be produced by the processor/exporter (where appropriate in collaboration with the processor/importer). The controller can rely on the assessment prepared by the processor and, if necessary, supplement it. For example, where the assessment received by the controller appears incomplete, inaccurate or raises questions, the should additional information, verify the information and complete/correct it if necessary, bearing in mind that the assessment must comply with EDPS recommendations 01/2020 and the steps outlined therein. This includes identifying relevant laws and practices in the light of all the circumstances of the transfer, and identifying appropriate additional measures if necessary".

[24] See the executive summary and §60 of EDPS Opinion 22/2024, *op. cit*, (French translation by CNIL): "Where transfers of personal data outside the EEA take place between two processors, in accordance with the controller's instructions, the controller remains subject to the obligations arising from Article 28(1) of the GDPR concerning "sufficient guarantees", in addition to those provided for Article 44 to ensure that the level of protection guaranteed by the GDPR is not called into question by transfers of personal data. The processor-exporter must prepare the relevant documentation, in accordance with case law and as explained in EDPS recommendations 01/2020. The controller must assess this documentation and be in a position to present it to the competent data protection authority. The data controller may rely on the documentation or information received from the subcontractor and, if necessary, supplement it. The extent and nature of the controller's obligation to assess this documentation may depend on the tool used for the transfer and whether the transfer constitutes an initial or a subsequent transfer". The EDPS also states that "data protection authorities should assess whether the controller is able to demonstrate that verification of the sufficiency of the guarantees provided by its processors (and subsequent subcontractors) has taken place to the 's satisfaction. The controller may choose rely on the information received from its processor and supplement it where necessary (for example, where it appears incomplete, inaccurate or raises questions). More specifically, for processing operations 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 AITD perimeter and consideration of subsequent transfers

The first step in creating the DTIA is to map data transfers (see step 1 of this guide). This mapping involves clearly identifying the data importer and the third country of import. It enables the data exporter (and *ultimately* the data controller, if the transfer is not carried out by the latter) to identify the additional measures to be put in place (see steps 4 and 5 of this guide).



The exporter's analysis must take into account the entire data flow, including subsequent transfers, so that the controller (whether or not it is the exporter) can assess the risks associated with all data transfers outside the EEA[25].

A DTIA may concern a single transfer or a series of transfers. Consequently, the exporter has the choice of documenting his analysis within the same or several documents. In the event of a change in the chain of transfers, he can modify the existing analysis or create a new one.

[25] In §97 of his Opinion 22/2024, the EDPS states that "*data controllers must be able to present documentation relating to [onward] transfers. This means that the controller must receive this information from the exporting subcontractors or exporting subsequent subcontractors, showing that the importers are indeed complying with the requirements for subsequent transfers as set out in the transfer tool*".

analysis that he can link to pre-existing analyses he has already carried out. If the exporter is a subcontractor, he must share this information with the data controller.

Furthermore, any subsequent transfer is subject to the importer's compliance with the obligations laid down in transfer tool used. If Commission standard contractual clauses (STC)[26] have been agreed, the data importer not to disclose the personal data to a third party located outside European Union in the same country as data importer or in another unsuitable third country (hereinafter "onward transfer"), unless the third party is bound by the STC or agrees to be bound, by virtue of the appropriate module. Otherwise, a onward transfer by the data importer can only take place if the conditions laid down in the TCCs are met (module 1, article 8.7 and 8.8; modules 2 and 3 - article 8.8) and on condition that he complies with his obligations to maintain the documentation necessary to demonstrate his compliance (modules 1 and 3, article 8.9; module 2 - article 8.8).

2.5 Compliance of the transfer with the principles of the RGPD

A data transfer, like any other processing operation, must comply with all the principles of the RGPD. In accordance with Article 5 of the RGPD, the data controller must (directly if is itself the exporter, or through its processor if it is the exporter) in particular ensure that the transfer is lawful and based on one of the legal grounds set out Article 6 and, where applicable, Article 9 of the RGPD. Data must also be adequate, relevant and limited what is necessary for the purposes for which it is processed. It is therefore necessary to ensure that the data transferred is limited to what is strictly necessary in view of 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 anonymized data instead of personal data, while ensuring that the anonymization process is implemented in accordance with the EDPS guidelines[27]. In this case, the GDPR does not apply.

3. The different stages of AITD

To perform an AITD, we recommend the following 6 steps:

3.1 Getting to know your transfer (step 1)

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

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

You can also contact data importer.

[26] See the standard contractual clauses published by the European Commission: https://commission.europa.eu/system/files/2021-06/1_fr_annexe_acte_autonome_cp_part1_v4.pdf

[27] For more details on anonymization, see Article 29 Working Party (G29), Opinion 05/2014 on Anonymization Techniques: https://www.cnil.fr/sites/cnil/files/atoms/files/wp216_fr.pdf, as well as dedicated articles on the CNIL website, including "Anonymization of personal data": https://www.cnil.fr/fr/technologies/lanonymisation-de- donnees-personnelles; Work is currently underway within the EDPS to publish new Anonymization Guidelines.

Exporter	
Name exporter	
Point of contact and contact details (internal department or person responsible for the transfer)	
Data export country	
Qualifying the exporter in the context of data transfer[28]	☐ Data controller ☐ Joint controller ☐ Subcontractor *If "**Subcontractor**" or "**Joint Controller**", specify the name of the controller or other joint controllers:*
Any other useful information	

Importer	
Importer's name	
Point of contact and contact details (internal department or person responsible for the transfer)	
Data import country	
Importer qualification in the data transfer context	☐ Data controller ☐ Joint controller ☐ Subcontractor *If "**Subcontractor**" or "**Joint Controller**", specify the name of the controller:*
Nature of importer's activities[29]	*Specify type :*

[28] See EDPS, Guidelines 07/2020, op.cit.
[29] Information help identify the legislation applicable in the third country.

Importer	
	Is specifically protected data importer? *by legislation of the country of destination of the data [30]?*
Any other useful information	

Transfer	
Importer's processing activities on transferred data (*e.g. computer support, marketing, supply of software in cloud, data hosting*)	
Transfer type (*how data is made available to the importer*)	☐ **Remote access without local download/storage** - data is hosted by the exporter within the EEA. The importer cannot download copies of the data, but can access it remotely from an unsuitable country outside the EEA. ☐ **Remote access local download/storage option** - data is hosted by the exporter within the EEA. The importer has the option of accessing the data from a third country and, if necessary, downloading and storing copies of the data in a country outside the EEA which is not suitable. ☐ **Transmission and local hosting / storage** - The importer hosts or stores personal data in a non-EEA country that is not adequate. ☐ **Other**
Transfer method (*e.g. transmission by secure file transfer protocol (SFTP), transmission by e-mail, connection via an application programming interface (API), connection to a remote server, storage of data in a physical medium and dispatch, etc.*).	
Data transfer format	☐ In plain English ☐ Figures

[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, EDPS, Recommendations 01/2020 on measures to complement transfer instruments designed to ensure compliance with the EU level of personal data protection.

Transfer	
	☐ Pseudonymized ☐ Other *If "**Other**, specify :*
Transfer frequency	☐ Single transfer ☐ One-time / occasional transfer (*recurrence to be specified*) : ☐ Regular transfer (*recurrence to be specified*) :
Possibility of subsequent transfers for the importer *(see section 2.4 above)*	☐ Yes ☐ No *If **yes**, please specify :*
Categories of personal data transferred	☐ Identification (*please specify*) : ☐ Contact details *(please specify)* : ☐ Details of family life (*please specify*) : ☐ Details of professional life (*please specify*) : ☐ Service usage (*please specify*) : ☐ Other (*please specify*) :
Special categories of personal 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 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 an individual's sex life (*please specify*) : ☐ None of the above
Other highly personal data transferred	☐ Data on criminal convictions and offences[31] (*please specify*) :

[31] Article 10 of the RGPD

Transfer	
	☐ National identification number[32] (*please specify*) : ☐ Geolocation data[33] (*please specify*) : ☐ Financial data likely be used for fraudulent payments[34] (*please specify*) : ☐ Other (*please specify*) : ☐ None of the above
Categories of people concerned	
Vulnerable persons among those concerned (*e.g. minors, dependent persons)*	☐ Yes ☐ No *If "**Yes**", specify :*
Total or partial transfer[35] (if relevant)	☐ Total ☐ Partial *If "**partial**", specify percentage (if possible) :*
Volume of data transferred (if possible)	
Number of people concerned (if possible)	
Proposed start date of transfer (if possible)	
Proposed end date or duration transfer (if possible)	

[32] Article 87 of the RGPD
[33] See Article 29 Working Party (G29), Guidelines on data protection impact assessment DPIA) and how to determine whether processing is "likely result in a high risk" for the purposes of Regulation (EU) 2016/679, p.11: https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf
[34] Idem
[35] Transferred data represents all or part of the processed data.

3.2 Identify the transfer tool used (step 2)

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

Article 46 RGPD transfer tool	
Article 46 transfer tool used to support the transfer	☐ Standard Contractual Clauses (SCC)[36] (Module used to be specified) : ☐ Binding corporate rules (BCR) for data controllers[37] ☐ Binding corporate rules (BCR) for subcontractors[38] ☐ Code of conduct[39] ☐ Certification mechanism[40] ☐ Ad hoc contractual clauses
Elements and documentation attesting to transfer tool in place (e.g. contract signed with data importer, certification attestation from data importer, copy of BCR with list of entities covered by BCR including data importer)	

If the transfer is based on one of the transfer tools in Article 46 of the RGPD, it is necessary to carry out a AITD and proceed to step 3.

If it is not necessary to perform a DTIA (see section 2.2), it is recommended that the decision not to perform a DTIA be documented.

[36] See the standard contractual clauses published by the European Commission: https://commission.europa.eu/system/files/2021-06/1_en_annexe_acte_autonome_cp_part1_v4.pdf. In its FAQ on SCCs, the European Commission indicates that an additional set of SCCs, dedicated to transfers to importers subject to the RGPD is currently developed. Once this new set is adopted, it will be possible to use it to frame transfers to importers subject to the RGPD. See §25 of the European Commission's FAQ on CCTs: https://commission.europa.eu/law/law-topic/data-protection/international- dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#scope-of-application-and-transfer- scenarios

[37] For , see EDPS, Recommendations 1/2022 concerning the application approval and the elements and principles of binding business rules for controllers (Article 47 of the RGPD): https://www.edpb.europa.eu/system/files/2024-05/edpb_recommendations_20221_bcr-c_v2_fr.pdf

[38] For BCR-Subcontractor, see G29, instruction form WP265: https://www.cnil.fr/sites/cnil/files/atoms/files/wp_265-bcr-st- formulaire-en.doc; and approval reference WP257: https://www.cnil.fr/sites/cnil/files/atoms/files/wp-257_bcr-st- referentiel_en.pdf.

[39] See EDPS, Guidelines 04/2021 on codes of conduct as tools for transfers: https://www.edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_fr.pdf

[40] See EDPS, Guidelines 07/2022 on certification as a transfer tool (version 2.0): https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_fr_0.pdf

3.3 Evaluate legislation and practices in the country of data destination and efficiency of the transfer tool (step 3)

Once a clear picture of the transfer and the tool used to manage it has been obtained, the third step is to determine whether there are any elements in the legislation or practices of the importing third country that could undermine the effectiveness of the guarantees of the tool used, in the specific context of the transfer, or prevent the exporter or importer from fulfilling their obligations[41]. The description of the transfer (in step 1) enables its characteristics and sensitivity to be taken into account in the assessment of the legislation and practices of the country of destination of the data, and of effectiveness of the transfer tool (step 3).

The importer's cooperation is essential for this exercise: it is up to the exporter to ask him to provide an analysis of his legislation, particularly in terms of access to data by the authorities, or *at the very least* to provide a list of the applicable laws. It is therefore important to involve the importer in carrying out the DTIA, insofar as the importer must comply with the instructions of the exporter and the data controller (if the exporter is a subcontractor).

To complete this step, it is recommended to Annex 3 of EDPS recommendations on additional measures[42], which lists, in a non-exhaustive way, sources of information that can be used. These sources must be relevant, objective, reliable, verifiable and publicly available or otherwise accessible.

You can use the CNIL world map, which contains information on the data protection framework in the third country (existence a data protection law and a data protection authority).

When analyzing legislation access to data by public authorities, we should not hesitate to draw on reports by international organizations and expert analyses, such as those commissioned by the EDPS for certain countries[43]. These analyses should be supplemented and updated as necessary.

It is advisable to share analyses through networks of DPOs, professional federations and groups of companies or administrations.

Data protection legislation	
Which is the frame **applicable à the importer** in terms of data protection?	*Text reference :*

[41] more information on how to assess this, please refer to §43.3 of EDPS recommendations 01/2020 on measures to complement transfer tools designed to ensure compliance with the EU level of personal data protection: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[42] See the measures that complement the transfer tools designed to ensure compliance with the level of protection of personal data. EU staff in .

[43] The EDPS has commissioned expert on:

- Russia, India, China (https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf);
- the Brazil (https://www.edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf) ;
- the Mexico and the Turkey (https://www.edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_mexico_and_turkiye_final_report_milieu_redacted.pdf).

Data protection legislation		
Which is its field application?	☐ General framework ☐ Sector application	*If sectoral application, specify :*
Third country's accession to international data protection treaties	☐ Yes ☐ No	*If yes, please specify :*
Is there a competent data protection authority (or an administrative body with comparable prerogatives) in the third country?	☐ Yes ☐ No	*Name authority :*
this authority/entity independent[44]?	☐ Yes ☐ No	*Justify :*
What are the rights of the people concerned?	**Rights of persons concerned**	
	Right of access ☐ Yes ☐ No	*If yes, reference :*
	Right of rectification ☐ Yes ☐ No	*If yes, reference :*
	Right of deletion	*If yes, reference :*

[44] In order to determine whether the authority is independent, it is possible to rely on Articles 52 to 54 of the GDPR, Article 15 Council of Europe Convention 108+ (https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726), as well as the work of the Global Privacy Assembly (GPA), all three of which are available in English:

- Article 5.1 of its rules of procedure: https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-Rules-and-Procedures-October-2020.pdf ;
- Principle B.2 of its accreditation principles: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Accreditation-Features-of-Data-Protection-Authorities.pdf; and
- the document from the Working Group on the Future of the Conference "Interpretation of the criteria of autonomy and independence": https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence- criteria_post-Coe-comment.pdf.

It is also possible to draw on the more general work of the Organisation for Economic Co-operation and Development (OECD):

- "Being an Independent Regulator, The Governance of Regulators (available in https://www.oecd.org/en/publications/being-an-independent-regulator_9789264255401-en.html ;
- "Create a a culture of independence : Guidelinesguidelines for counter undue https://www.oecd.org/fr/publications/creer-une-culture-d-independance_9789264287884-fr.html

Data protection legislation		
	☐ Yes ☐ No	
	Right object in specific situations ☐ Yes ☐ No	*If yes, reference :*
	Right object to automated decision-making ☐ Yes ☐ No	*If yes, reference :*
	Other rights ☐ Yes ☐ No	*If yes, please specify :*
	Are the restrictions on these rights necessary and proportionate in a democratic society? ☐ Yes ☐ No	*If yes, please specify :*
Tracks of remedies and penalties	Are there any effective means of redress? ☐ Yes ☐ No	*Justify :*
	Are penalties effective and dissuasive? ☐ Yes ☐ No	*Justify :*
	Can these rights and remedies be exercised by nationals of EEA member states? ☐ Yes ☐ No	*Justify :*
Laws and/or practices access to data		
Are there any supervisory laws **applicable to the importer** establishing obligations to disclose data to	*If yes, list :*	
	References	*Description (scope of application, public authority*

		concerned,
Data protection legislation		
personal transferred or grant access to such data to public authorities[45]? ☐ Yes ☐ No		*nature of the obligation, etc.)*
Are there any monitoring **applicable to theimporter** entailing obligations to disclose transferred personal data or to grant personal data transferred or to grant		

[45] These laws may be general in scope, concerning the application of criminal law or the protection of national security. They may concern authorities such as government bodies, regulators, tax authorities, the police, intelligence agencies and so on.

Data protection legislation		
access to these data to public authorities[46]? ☐ Yes ☐ No		
Essential warranties[47]		
Is access to data governed by clear, precise and accessible rules? ☐ Yes ☐ No	*Justify :*	
Is access to the data necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the RGPD[48]?	*Justify :*	

[46] *Idem*.
[47] See EDPS Recommendations 02/2020 on European essential safeguards for surveillance measures: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
[48] 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 protection against and prevention of to public security ; (eother important objectives general public interest of the Union or a Member State, in particular an important economic or financial interest of the Union or a Member State, including monetary, budgetary and taxation matters, public health and social security; (f) the protection of independence of justice and legal proceedings; (g) the prevention, detection, investigation and prosecution of breaches of ethics in the 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 of the rights and freedoms of others; (j) the enforcement of civil law claims.

Data protection legislation		
☐ Yes ☐ No		
Is access to data controlled by a independent monitoring mechanism? ☐ Yes ☐ No	*Justify :*	
Is the public authority concerned subject to transparency and regular control obligations? ☐ Yes ☐ No	*Justify :*	
Does the person concerned have general (not subject to nationality requirements) and effective remedies before an independent and impartial body? ☐ Yes ☐ No	*Justify :*	

Rule of law		
Are there any rule of law issues affecting the ability of data subjects to seek redress against unlawful access to personal data? ☐ Yes ☐ No	*If yes, list :*	
	Problem	*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 been the subject of direct access by the authorities of a third country to the personal data of nationals of an EEA member state (at least in recent years)? ☐ Yes ☐ No	*If **so**, specify how this can be demonstrated[49] :* *If **no**, specify here the type of requests received, the quantity and the way in which they were processed and/or the reasons why you think you may receive such requests in the future:*
Can it be demonstrated that there is no reason to believe that the importer will be subject to a request for access or direct access by the authorities of the third country, in particular because the legislation or problems identified will not apply in practice to the data transferred and to the importer (given its sector of activity and the history of requests for access from the authorities of the country third parties)[50]? ☐ Yes ☐ No In this case, it is possible to decide to proceed with the transfer without implementing any additional measures.	*If **so**, specify how this can be demonstrated[51] :*

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

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

[50] In certain 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 the importer, it may be possible to decide to proceed with the transfer anyway without implementing additional measures. It is then necessary to demonstrate and document this assessment, if necessary in collaboration with the importer, also taking into account the experience other players operating in the same sector and/or in sectors linked to similar transferred personal data other sources information. See EDPS, Guidelines 01/2020, §43.3

[51] For example, through information published other players operating in the same and/or related sectors.

☐ 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, and it is decided to proceed with the transfer without implementing additional measures (3).

Justify :

If the conclusion is (1) that the transfer tool is effective in the light of the assessment carried out or (3) that, despite the ineffectiveness of the tool, it is possible to proceed with the transfer without implementing additional measures, it is possible to proceed with the transfer. Step 6 is recommended.

If the conclusion is that (2) the transfer tool is not effective in the light of the assessment carried out, it is necessary go step 4 to identify additional measures.

3.4 Identify and adopt additional measures (step 4)

It is necessary identify on a case-by-case basis which additional measures might be effective for the transfer to a given third country. In particular, the description of the transfer in step 1 enables its characteristics and sensitivity to be taken into account when assessing the additional measures to be put in place. The greater the risk to the rights and freedoms of data subjects, the greater the checks to be carried out and the additional measures to be put in [place52].

These measures are referred to as "additional", as they complement the transfer tool designed ensure compliance with the EEA's level of personal data protection. It is therefore necessary to list in the table below both measures already , where applicable, and newly identified measures.

Annex 2 of the EDPS recommendations on additional measures provides a non-exhaustive list of technical, contractual and organizational measures that can be implemented in the form of use cases. It also presents use for which the is unable to identify effective [measures53].

It may be necessary to combine several additional measures. In most , contractual and organizational measures are not sufficient to prevent possible access to data by third-country authorities, and must be supplemented by duly implemented technical [measures54].

The effectiveness of additional measures may vary depending on the transfer described in step 1 and on the third country, hence the importance of carrying out a detailed analysis in step 3. **In some cases, the conclusion will be that no additional measures can ensure a level of protection essentially equivalent to European law for the transfer in question, which should lead to the data transfer in question not being carried out.**

---

[52] In its opinion 22/2024, the EDPS states that "*for processing operations presenting a high risk to the rights and freedoms of data subjects, the controller should increase its level of verification in terms checking the information provided*". With regard to transfers specifically, it states, "*the obligation for the controller to verify whether processors ([including] subsequent processors) present sufficient guarantees to implement the measures [it has] determined under Article 28(1) of the GDPR should apply regardless of the risk to the rights and freedoms of data subjects. Nevertheless, the extent of this verification will vary in practice depending on the nature of the organizational and technical measures determined by the controller on the basis, among other criteria, of the risk associated with the processing*." See EDPS, Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), executive summary, §60 and 83.

[53] See EDPS, Recommendations 01/2020, use 6 and 7, §93 to 97.

[54] See EDPS, Recommendations 01/2020 , §53: "*Contractual and organizational measures alone will not generally overcome access to personal data by third-country public authorities on the basis of problematic legislation and/or practices. Indeed, in certain situations, only duly implemented technical measures could prevent or render inoperative access by third-country public authorities to data, in particular for surveillance purposes*".

This process of identifying additional measures should be undertaken with due diligence, in collaboration with the importer, and should be documented. The involvement of the information systems manager is essential. It is recommended to append to the DTIA the opinions or analyses of the persons or entities that have been consulted (e.g. DPO, legal and technical counsel, information systems manager, data protection authority).

Existing additional measures			
Description (For each measure, provide a description, specify whether it is implemented by the importer or exporter and to what extent it complies with the EDPS recommendations)			**Impact of measures** (For each measure, specify which risk(s) is/are mitigated)
Technical measures	☐ Pseudonymization55 ☐ Encryption56		

[55] See EDPS Recommendations 01/2020, use case 2, §85 :

1. *A data exporter transfers personal data in such a way that it can no longer be attributed to a specific data subject or used to distinguish the data subject within a group, without recourse to additional information.*
2. *the additional information is held exclusively by the data exporter and stored separately in a Member State or in a third country by an entity trusted by the exporter in the EEA or in a jurisdiction offering a level of protection essentially equivalent to that guaranteed in the EEA,*
3. *unauthorized disclosure or use of such additional information is prevented by appropriate technical and organizational safeguards, and it is ensured that the exporter retains exclusive control of algorithm or directory enabling re-identification using the additional information, and*
4. *the controller has established, by means a thorough analysis of the data in question, into account all the information which the public authorities of the recipient country may have at their disposal and which they may use, that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person even by cross-checking with such information*

[56] See EDPS Recommendations 01/2020, use case 3, §90 :

1. *A data exporter transfers personal data to a data importer in a jurisdiction where legislation and/or practice allow public authorities to access the data while it is being transmitted over the Internet to that third country without the essential European safeguards relating such access, encryption of the transmission is used, ensuring that the encryption protocols employed are state-of-the-art and offer effective protection against active and passive attacks using resources known to be available to the third country's public authorities,*
2. *the parties involved in the communication agree on a trustworthy public key certification authority or infrastructure,*
3. *specific, state-of-the-art protection measures are used against active and passive attacks on the sending and receiving systems encrypt transmission, including software vulnerability tests and possible backdoors,*
4. *if transfer encryption in itself does not provide sufficient security due to the vulnerability of the infrastructure or 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 or operating mode, where applicable) comply with the state of the art and can be considered resistant to cryptanalysis by public authorities when the data is transited 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 length of time during which the confidentiality of encrypted personal data must be preserved,*
7. *the encryption algorithm is correctly executed by duly software, with no known vulnerabilities, and whose compliance with chosen algorithm specification has been verified, for example by certification,*

Existing additional measures			
	☐ Other (specify) :		
Organizational measures [57]	☐ Documentation of access requests (requests received, response, legal reasoning, players involved) ☐ Data minimization (strict and granular access, confidentiality policies, access on a need-to-know basis, control through audits, disciplinary measures) ☐ Governance (information and involvement of the data protection delegate or RGPD referent all access requests) ☐ Adoption of security and data protection standards (certification and compliance safety standards) ☐ Internal policies and procedures for handling access ☐ Division of responsibilities between entities within the same group, designation of specific teams to handle access requests, training of personnel responsible for managing these requests. ☐ Other (specify) :		
Contractual measures [58]	☐ Inclusion of additional technical or organizational measures in a binding contract ☐ Transparency obligation ☐ Importer's obligation to enumerate the laws		

8. the keys are reliably managed (generated, administered, stored, where appropriate linked to identity of the intended recipient and deleted) by the exporter or by an entity trusted by the exporter located in a territory offering a substantially equivalent level of protection

[57] See EDPS Recommendations 01/2020, Section 2.3 Organisational measures, § 128 to 143 :

[58] See EDPS Recommendations 01/2020, Section 2.2 Additional contractual measures, §98 to 127.

Existing additional measures			
	practices, measures to prevent access, requests for access, and whether it is legally prohibited from providing the aforementioned information - Prohibition on the use of backdoors or processes that facilitate access to data - Can audited to verify compliance - Notification to exporter (and data subjects) in event of access to data public authorities - Commitment to contest access requests - Undertaking by the importer to review the legality of any disclosure order and to challenge it if there are grounds to do so - Undertaking to apply for interim measures to suspend the effects of the order until the court has ruled on the merits of the case - Undertaking to inform in the event of inability to meet contractual commitments - Sanctions in the event of violation, including compensation for the persons concerned - Termination of contract in event of failure to comply with data transfer obligations - Undertaking by the importer to provide the authorities of the third country with only the minimum amount of information when responding to a request for access. - Undertaking by the importer to inform the authority of the third country incompatibility with data protection laws, and		

Existing additional measures			
	to be notified simultaneously the exporter ☐ Unencrypted data can only be consulted with the explicit or implicit consent of the exporter. ☐ Other (specify) :		
Conclusion		☐ The transfer tool, combined with these existing measures, **is effective in** the light of the evaluation carried out. ☐ The transfer tool, combined with these existing measures, **is not effective in** the light of the evaluation carried out. In such cases, additional measures need to be considered.	

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

If the conclusion is that the transfer tool, combined with these measures, **is effective in** the light of the evaluation carried out, then transfer is possible, subject to the effective implementation of all the necessary additional measures. If existing measures are sufficient, we can proceed directly to step 6. If additional measures are required (over and above those already in place), we recommend that you proceed to step 5.

Following completion of DTIA, or at time of a reassessment, if the conclusion is that it is not possible 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 , it must be stopped.** Go to

In the latter case, the importer must erase all data and provide proof of this to the exporter, or the exporter to the importer.
restore all data and delete existing copies.

3.5 Implement additional measures (step 5)

Once the appropriate additional measures to ensure that the transferred data enjoys an essentially equivalent level of protection have been identified, it is advisable to list in the table below the actions to be taken concerning the additional measures still to be put in place and compliance with any procedural steps to be followed. This will help ensure their effectiveness and anticipate any obstacles (e.g. financial difficulties, unavailability of competent teams, etc.).

The procedural steps to be followed may vary according to the transfer tool on which the transfer is based. The EDPS recommendations on additional measures list some of these steps[59].

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

[59] See, EDPS, Recommendations 01/2020, section 2.5 Step 5, §59 to 68. For example, the need for the exporter to request authorization from the competent authority in cases where the CCTs have been modified and this restricts rights and obligations they contain, or where the additional measures contradict the CCTs.

Opinions
Opinion of the person in charge of data protection (or data protection delegate, if applicable)
Opinion of the person in charge of information system security (or the person responsible information system security, if applicable)

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

3.6 Reassess at appropriate intervals (step 6)

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

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 protection of the transfer before the initial date of the next review, for example in the event of a change in the legislation or practices of the third country, the importer's inability to meet its commitments, or a change in the European Commission's assessment of the law applicable in the third country. To this end, it is advisable to keep abreast of legislative developments in the country in question, so as to be able to anticipate any need to reassess data protection in that country.

Reassessing protection	
Interval between reviews (e.g. every 2 years)	
Date of next issue	
Early review, if applicable, and justification for anticipation	