DRAFT PRACTICAL GUIDE

TRANSFER IMPACT ASSESSMENT

DRAFT

Draft guide for public consultation until February 12th, 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Introduction

1.1 Context

Regardless of their status (public or private, profit-making or non-profit) or their size (multinational companies or medium and small businesses, artisans or self-employed professionals), a large number of controllers and processors are concerned by the issue of transfers. The interpenetration of networks and the development of cross-border services (in particular cloud services) have increased the number of occasions on which personal data (hereinafter referred to simply as "data") is processed in whole or in part in third countries that are not subject to European Union (EU) law (and in particular to the GDPR), thus giving rise to transfers.

Yet, the principle enshrined in the GDPR is that in the event of a transfer, the data must continue to benefit from the same level of protection as the one offered by that text. Indeed, Recital 101 of the GDPR states that it is important 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 on data transfers.

In its so-called "Schrems II" ruling[1], the Court of Justice of the European Union (CJEU) emphasised the responsibility of exporters and importers to ensure that personal data is processed, and continues to be processed, in compliance with the level of protection set by the 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, in a position to comply with its personal data protection commitments. Exporters relying on Article 46 GDPR tools for their personal data transfers are therefore obliged to assess the level of protection in the third country of destination of the data and the need to put in place additional safeguards. Such assessment is commonly known as a Transfer Impact Assessment (TIA).

1.2 The Necessity to Carry Out a TIA

A TIA must be carried out by controllers or processors acting as exporters, with the assistance of the importer, prior to transferring data from a European Economic Area (EEA) country[2] to a third country where that transfer relies on an Article 46 GDPR tool. If the country of destination is covered by an adequacy decision by the European Commission, the exporter is not subject to this obligation. The same applies if the transfer is carried out on the basis of one of the derogations listed in Article 49 of the GDPR.

In cases where the transfer of data is indispensable, the purpose of the TIA is to assess whether the importer will be able to comply with its obligations as set out in the transfer instrument in place, in light of the legislation and practices of the third country of destination - in particular with regards to potential access to personal data by the third country authorities -, and to document this assessment. To this end, the exporter must assess the level of protection offered by the local legislation and consider the practices by the authorities of the third country in light of the planned transfer. If necessary, the TIA should enable the exporter to assess whether supplementary measures would make it possible to remedy the shortcomings identified in the data protection and ensure the level required by EU legislation. As the importer holds a lot of information required for this assessment, its cooperation is essential for the TIA to be carried out. In the context of a relationship between a controller and a processor, the transmission of this information to the controller by the processor is part of the latter's obligations under Article 28 of the GDPR, and in particular under Article 28(3)(h). It should be noted that the transmission by the processor of a simple conclusion or an executive summary of its assessment, without the provision of concrete information on the legislation of the third country and the practices of the authorities, as well as on the circumstances of the transfer, does not enable the processor to fulfil its obligations under Article 28 of the GDPR.

In line with the recommendations of the European Data Protection Board (EDPB) on measures that supplement transfer tools[3], the CNIL has drawn up this guide to help exporters carry out their TIA.

---

[1] Judgment of the Court (Grand Chamber) of 16 July 2020, "Schrems II", C-311/18

[2] The European Economic Area (EEA) is made up of the Member States of the European Union, as well as Norway, Iceland and Liechtenstein, to which the GDPR is applicable by incorporation into the EEA Agreement.

[3] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

DRAFT

1.3 The Aim of This Guide

This guide constitutes a methodology, a checklist, which identifies various elements to be considered when carrying out a TIA. It gives indications on how the analysis can be carried out by following the six steps set out in EDPB's recommendations, and points to the relevant documentation. It does not constitute an evaluation of the laws and practices in the third country and risks related thereto.

Therefore, if you are a controller or processor and you are considering transferring personal data, below you will find the main elements to be considered in order to carry out your analysis and ensure that the level of personal data protection in the third country is sufficient.

The use of this guide is not obligatory. Other elements can be considered and other methodologies can be applied.

This guide is organised in six different steps to be followed to carry out a TIA:

1. **Know your transfer**
2. **Document the transfer tool used**
3. **Evaluate the legislation and practices in 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 and the necessary procedural steps**
6. **Re-evaluate at appropriate interval the level of data protection and monitor potential developments that may affect it**

Step 1 enables the exporter to describe the transfer so that its characteristics and sensitivity can be considered in the assessment.

Step 2 involves documenting the tool that will be used for the transfer and the analysis concluding whether or not a TIA is required for it.

Step 3 enables the exporter to assess the legislation and practices in the country of destination of the data and to identify whether there are any factors that could impinge on the effectiveness of the guarantees provided by the transfer tool used (step 2).

Step 4 consists of identifying the existing security measures (technical, contractual and organisational) that ensure a sufficient level of data protection in the third country, considering the transfer (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 supplementary measures that need to be implemented to ensure that the data transferred enjoys a level of protection in the third country that is substantially equivalent to that afforded within the EEA.

Step 5 contains a model action plan for the operational implementation of the additional measures identified in step 4.

Finally, **step 6** allows the exporter to anticipate future reassessments of the transfer.

DRAFT

2. Before Carrying Out a Transfer Impact Assessment

To determine whether a TIA is necessary, several elements are to be considered.

1. Is the data in question 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 "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"[4].

2. Is there a transfer of personal data?

The EDPB has identified, in its guidelines[5], the following three cumulative criteria that establish whether a processing operation can be qualified as a transfer:

A controller or a processor ("exporter") is subject to the GDPR for the given processing;

The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer");

The importer is in a third country (outside the EEA), irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.

The two entities must therefore be legally distinct and each of them must be either a controller, a joint controller or a processor. Chapter V of the GDPR therefore does not apply to the transmission or provision of data internally within the same structure. This means that a scenario in which an employee of a controller in the EU remotely accesses his employer's database from a third country, during a business trip for example, does not constitute a transfer within the meaning of the GDPR. However, the transmission or provision of data between two entities belonging to the same group does constitute a transfer. You should bear in mind that remote access from a third country to data stored in the EEA and/or cloud storage of data outside the EEA constitutes a transfer.

3. What is the qualification of the actors implicated?

The qualification (controller, joint controller or processor) of the various entities involved in the transfer must be clarified, as it determines the allocation of responsibilities and may entail different obligations for the two parties. To help you with this analysis, information is available on the CNIL's website[6]. The EDPB has also produced guidelines[7] dedicated to these concepts.

4. Does the transfer comply with all the principles of the GDPR and, in particular, can you minimise the amount of personal data transferred or transfer anonymised data rather than personal data?

When transferring data, as with their other processing activities, the exporter must comply with all the principles of the GDPR. In accordance with Article 5 of the GDPR the exporter shall notably ensure that the transfer in question has a legal basis.

In addition, data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed. You must therefore ensure that the data transferred is limited to what is strictly necessary for the purposes for which it is transferred. You should also consider disclosing or transmitting anonymised data instead of personal data where possible, while ensuring that the anonymisation process is operated effectively and prevents any re-identification[8].

DRAFT

---

[4] See, for example the different resources on the CNIL's website here and here

[5] See EDPB 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.

[6] See, for example the dedicated page on the CNIL's website available in French

[7] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR

[8] For more details on anonymisation, see Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, as well as the dedicated articles on the CNIL website available in French

You must ensure that data subjects have been informed in accordance with articles 13 and 14 of the GDPR.

5. Can your data be 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[9] do not require the implementation of supplementary measures. If you are thus able to transfer personal data to such a country, this will ensure an adequate level of protection for the data in question. In this case, you will not need to carry out a TIA.

Please note that adequacy decisions may have a limited scope (for example, Canada's adequacy decision[10] only applies to private sector organisations that process personal data in the course of commercial activities) or concern only certain self-certified entities in the concerned country (for example, self-certified entities under the adequacy decision for the United States[11]). **It is therefore up to you to check that the planned transfer is covered by the adequacy decision.**

You should also bear in mind that adequacy decisions are subject to periodic review. You should therefore regularly check the list of countries that have been the subject of an adequacy decision in case new decisions have been adopted, or countries have been removed from the list.

After these preliminary questions, if you consider that it is necessary to transfer personal data to a country that has not been the subject of an adequacy decision, this guide will help you to carry out your Transfer Impact Assessment.

DRAFT

[9] For the full list of countries covered by an adequacy decision, see the dedicated webpage of the European Commission.

[10] Commission Decision 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 (notified under document number C (2001) 4539)

[11] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C (2023)4745)

3. The Different Steps of the TIA

Step 1 – Know Your Transfer

In order to ensure an essentially equivalent level of protection for the data transferred, wherever it is being processed, first it is necessary to describe the transfer.

To complete the table below, you can use your pre-existing internal documentation, such as the record of processing activities or the contract governing the transfer. You can also contact the data importer.

Step 1: Know Your Transfer	
Exporter Name	
Contact Point and Contact Details	
Exportation Country	
Exporter Qualification in the Context of the Data Transfer[12]	☐ Controller ☐ Joint Controller ☐ Processor *If "**Processor**" or "**Joint Controller**", provide the name of the Controller:*
Importer Name	
Contact Point and Contact Details	
Importation Country	
Importer Qualification in the Context of the Data Transfer	☐ Controller ☐ Joint Controller ☐ Processor *If "**Processor**" or "**Joint Controller**", provide the name of the Controller:*
Nature of the Data Importer's Activities	☐ Commercial ☐ Public sector ☐ Non-profit ☐ Other *If "**Other**", specify:*

[12] See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

DRAFT

Step 1: Know Your Transfer	
Transfer Start Date	
Intended Transfer End Date or Transfer Duration	
Transfer Purpose(s) and Processing Activities Undertaken by the Importer Regarding the Transferred Data (e.g. IT support, marketing, provision of cloud software, data hosting)	
Transfer Type *(How is the data made available to the importer?)*	☐ **Remote access without the possibility to download/ locally store the data** - Personal data is hosted by the Exporter within the EEA. The Importer cannot download copies of the personal data, but the Importer can access the personal data remotely from a country outside the EEA not covered by an adequacy decision ☐ **Remote access with the possibility to locally download/store the data** - Personal data is hosted by the Exporter within the EEA, the Importer can access the personal data remotely from a country not covered by an adequacy decision, and if necessary, download and store copies of the personal data within the country outside of the EEA not covered by an adequacy decision. ☐ **Transmission and local storage/hosting** - The Importer hosts or stores the personal data in a country outside the EEA not covered by an adequacy decision.
Transfer Method (e.g.: email, secure file transfer protocol, remote access)	
Transferred Data Format	☐ *Plain text* ☐ *Encrypted* ☐ *Pseudonymised* ☐ *Other* *If "**Other**", please provide details:*
Transfer Frequency	☐ One-off transfer ☐ Occasional transfers ☐ Regular transfers
Possibility of Onward Transfers by the Importer	☐ Yes ☐ No *If "**Yes**", conduct a separate TIA dedicated to each onward transfer.*
Categories of Data Transferred	
Special Categories of Data Transferred ("Sensitive Data")	☐ Personal data revealing racial or ethnic origin ☐ Personal data revealing political opinions

DRAFT

Step 1: Know Your Transfer	
	☐ Personal data revealing religious or philosophical beliefs ☐ Personal data revealing trade union membership ☐ Genetic data and biometric data processed for the purpose of uniquely identifying a natural person ☐ Health data ☐ Data concerning a natural person's sex life or sexual orientation ☐ None of the above
Other Types of Sensitive or Highly Personal Data Transferred	☐ Personal data relating to criminal convictions and offences ☐ National identification number ☐ Geolocation data ☐ Payment data ☐ Other ☐ None of the above If "**Other**", please provide details:
Categories of Data Subjects	
Vulnerable Data Subjects *(e.g.: children, dependent persons)*	☐ Yes ☐ No *If "**Yes**", specify:*

DRAFT

Step 2: Identify the Transfer Tool Used

The following table is intended to help you document the transfer tool used for the transfer in question, in order to confirm whether or not a TIA is required.

A transfer may be based on:

- an adequacy decision by the European Commission;
- one of the transfer tools listed in Article 46 of the GDPR; or
- a derogation in accordance with Article 49 of the GDPR. With regards to the latter, it should be recalled, as underlined in the EDPB recommendations on supplementary measures13, that "only in some cases you may be able to rely on one of the derogations provided for in Article 49 GDPR if you meet the conditions. Derogations cannot become "the rule" in practice, but need to be restricted to specific situations".

As indicated, **conducting a TIA is required only when one of the tools of Article 46 is used.**

Step 2: Transfer Tool Used and Documentation	
Adequacy Decision	
Is the country of destination the subject of an adequacy decision by the EU Commission currently in force? [14]	☐ Yes ☐ No *If "**Yes**", you must verify the scope of this decision, as described below.* *If "**No**", the transfer cannot be based on an adequacy decision and another instrument must be used.*
Does the adequacy decision cover the third country as a whole or only to a limited extent?	☐ The whole country is covered ☐ The decision covers a defined sector or list of entities to which the Importer or the transfer belong ☐ The decision covers a defined sector or list of entities to which the Importer or the transfer **do not belong** ***In the first two cases**, the Importer is covered by the adequacy decision for transfers to the third country. You can therefore rely on this adequacy decision for your transfer and **it is not necessary to carry out a TIA**.* *In the third case, **if the Importer is not covered by the scope of the adequacy decision**, the transfer cannot be based on this adequacy decision and it is **necessary to use another instrument**.*

[13] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

[14] For the full list of countries covered by an adequacy decision, see the dedicated webpage of the European Commission.

DRAFT

Step 2: Transfer Tool Used and Documentation	
Derogations (Article 49 RGPD)[15]	
Does any of the derogations of Article 49 apply?	☐ Explicit consent of the data subject ☐ Transfer necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request ☐ Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; ☐ Transfer necessary for important reasons of public interest ☐ Transfer necessary for the establishment, exercise or defence of legal claims ☐ Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent ☐ Transfer made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case ☐ Transfer necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. *If "**Yes**", there is no need for a TIA,* *If "**No**", another instrument must be used.*
Article 46 GDPR Transfer Tools	
Is one of the transfer tools of Article 46 used for the transfer?	☐ Standard Contractual Clauses (SCCs)[16] ☐ Binding Corporate Rules (BCRs) [17]

DRAFT

[15] Specific conditions apply to some of the derogations. It is therefore necessary to refer to Article 49 of the RGPD. See also, EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

[16] See the Standard Contractual Clauses published by the European Commission: In its FAQ on CCTs, the European Commission indicates that an additional set of Standard Contractual Clauses, dedicated to transfers to Importers subject to the GDPR, is currently being developed. Once this new set has been adopted, it will be possible to use it to regulate transfers to Importers already subject to the GDPR. See §25 of the Frequently asked questions on the new SCCs

[17] For the BCR-Controller, see the EDPB 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).

For the BCR-Processor, see the WP265 application form and the table with the elements and principles to be found in

Step 2: Transfer Tool Used and Documentation	
	☐ Code of Conduct [18] ☐ Certification Mechanism [19] ☐ Ad hoc Contractual Clauses If **yes**, a **TIA is required**.
Conclusion	
Evidence and documentation of the transfer instrument put in place	
Is it necessary to carry out a TIA?	☐ **Yes** ☐ **No**

If your transfer is based on an adequacy decision by the EU Commission or an Article 49 derogation, then you do not need to follow the next steps. **You are not obliged to carry out a TIA.**

If your transfer is based on one of the transfer tools listed in Article 46 of the RGPD, then you must carry out a TIA and **you should proceed to step 3.**

Step 3 –Assess the Laws and Practices in the Country of Destination of the Data and the Effectiveness of the Transfer Tool

Once you have a clear vision of your transfer and the tool you are going to use, the third step is to determine whether there are any indications that the laws and practices of the third country where the data is imported could impinge on the effectiveness of the appropriate safeguards you are putting in place, in the specific context of the transfer, or that could prevent you from fulfilling your obligations[20].

To complete this section, you can consult Annex 3 of the EDPB recommendations on supplementary measures[21], which lists, in a non-exhaustive manner, sources of information that may be used. These sources must be relevant, objective, reliable, verifiable and publicly available.

Step 3: Assess the Laws and Practices in the Country of Destination of the Data and the Effectiveness of the Transfer Tool				
Data Protection Legislation	What data protection framework **applies to the Importer?**	Text reference(s)		
		Scope	☐ General application ☐ Sectorial application	*If "**Sectorial application**", specify:*

Binding Corporate Rules

[18] See EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers

[19] See EDPB Guidelines 07/2022 on certification as a tool for transfers.

[20] For further information on how to assess this, refer to §43.3 of the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[21] See, EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

	What are the data subjects' rights and the redress mechanisms?	**Data Subjects' Rights**		
		Right of access	☐ Yes ☐ No	*If "**Yes**", add reference:*
		Right to rectification	☐ Yes ☐ No	*If "**Yes**", add reference:*
		Right to erasure	☐ Yes ☐ No	*If "**Yes**", add reference:*
		Other rights	*List here:*	
	Is there an independent data protection authority covering the material and geographical scope of the processing concerned?	☐ Yes ☐ No	*Name of the authority:*	
	Is this data protection authority independent?	☐ Yes ☐ No	*Justify:*	
	Are there effective and dissuasive remedies and penalties?	Effective remedies	*Justify:*	
		Effective and dissuasive penalties	*Justify:*	
Laws and practices that could impinge on the effectiveness of the transfer tool	Are there any laws or practices of surveillance **applicable to the Importer** establishing obligations to disclose the transferred personal data or to grant access to such data to public authorities?	☐ Yes No	*If "**Yes**", list and describe them here (reference, scope, public authority concerned, nature of the obligation, etc.):*	
	Are these laws and practices: (1) governed by clear, precise and accessible rules? (2) necessary and proportionate measures in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR[22] ?	Essential European guarantees[23] in the country of destination or access: Access to data is governed by clear, precise and accessible rules: ☐ Yes ☐ No Justify: Access is necessary and proportionate with regards to the legitimate objectives pursued:		

[22] These objectives are: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding 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 monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to 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 enforcement of civil law claims.

[23] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

DRAFT

	(3) monitored by an independent supervisory mechanism? subject to an effective challenge by data subjects?	☐ Yes ☐ No Justify: There is an independent supervisory mechanism and the public authority concerned is subject to obligations of transparency and regular monitoring: ☐ Yes ☐ No Justify: The data subject has general (not subject to nationality requirements) and effective remedies before an independent and impartial body: ☐ Yes ☐ No Justify:	
	Are there any rule of law issues affecting the ability of data subjects to challenge unlawful access to personal data?	☐ Yes ☐ No *If **yes**, you can list them below:*	
		Issue	**How does it affect the exercise of rights by data subjects?**
	Can the importer demonstrate that it has never been the subject of a request for access or direct access? Can the importer also demonstrate that it has no reason to believe that it will be (because the legislation or the problems identified will not apply in practice)?	☐ Yes ☐ No	*If **yes**, specify here how it can demonstrate this.* *If **no**, specify here the type of requests received, the quantity and the way in which they are dealt with and/or the reasons why it believes it may receive such requests in the future?*
Conclusion		☐ The transfer tool **is effective** in the light of the assessment of the local laws and practices. ☐ The transfer tool **is not** effective in the light of the assessment of the local laws and practices.	

If you conclude that the transfer tool is effective in the light of the assessment carried out, **you can proceed with the transfer**. You will need to complete step 6.

If you conclude that the transfer tool **is not effective** in the light of the assessment carried out, go to step 4 to identify additional measures.

Step 4 – Identify and Adopt Supplementary Measures

You must identify on a case-by-case basis which supplementary measures could be effective for the transfers in question towards the third country. It may be necessary to combine several supplementary measures. It should

DRAFT

be noted that, according to the EDPB's recommendations on supplementary measures, contractual and organisational measures are not sufficient in themselves to prevent possible access to data by the authorities of the third country. They must always be complemented by technical measures. These measures are referred to as "supplementary" in that they supplement the transfer tool used to ensure compliance with the EU/EEA level of protection for personal data.

You can thus list in the table below both measures already implemented, where applicable, and newly identified measures.

To assist you in this step, Annex 2 of the EDPB recommendations on supplementary measures provides a non-exhaustive list of technical, contractual and organisational measures that can be implemented in the form of use cases. It also presents use cases for which the EDPB has not been able to identify effective measures[24].

The effectiveness of supplementary measures may vary depending on the transfer described in step 1 and the third country, which is why it is important to carry out a detailed analysis in step 3. **In some cases, you may reach the conclusion that no supplementary measures can ensure a level of protection that is essentially equivalent to EU law for the transfer in question, which should lead you to avoid the data transfer in question.**

This process of identifying supplementary measures should be undertaken with due diligence, in collaboration with the importer and must be documented.

Step 4: Technical, Contractual and Organisational Measures		
Step 4A: Existing Measures		
Existing Measures		**Impact of the Measures**
Technical Measures *(e.g. encryption prior to transmission without access to plaintext data by the Importer, end-to-end encryption of data in transit without access to plaintext data by the Importer, transfer of pseudonymised data making it impossible for the Importer to identify the data subjects).*		
Contractual Measures *(e.g. inclusion of supplementary measures in the contract, transparency obligations, prohibition of the use of "backdoors", audit clause, notification of the Exporter in the event of access to data by the authorities, commitment to oppose access requests by the authorities, penalties in the event of breach of contract)*		

[24] See, use-cases 6 and 7 of the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Organisational Measures *(e.g. communication of a transparency report on access requests, data minimisation, compliance governance, obtaining certifications, implementation of internal policies and procedures)*		
Satisfaction with Existing Measures		☐ 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.

Step 4B: Supplementary Measures to be Implemented		
Supplementary Measures		**Foreseen Impact of These Measures**
Technical Measures *(e.g. encryption prior to transmission without access to plaintext data by the Importer, end-to-end encryption of data in transit without access to plaintext data by the Importer, transfer of pseudonymised data making it impossible for the Importer to identify the data subjects).*		
Contractual Measures *(e.g. inclusion of supplementary measures in the contract, transparency obligations, prohibition of the use of "backdoors", audit clause, notification of the Exporter in the event of access to data by the authorities, commitment to oppose access requests by the authorities, penalties in the event of breach of contract)*		
Organisational Measures *(e.g. communication of a transparency report on access requests, data minimisation, compliance governance, obtaining certifications, implementation of internal policies and procedures)*		
Satisfaction with Supplementary Measures		☐ The transfer tool, combined with these supplementary measures, **is**

	effective in the light of the assessment carried out. ☐ The transfer tool, combined with these supplementary measures, **is not effective** in the light of the assessment carried out.

If you conclude that the transfer tool, combined with these measures, **is effective** in the light of the assessment carried out, you can implement the transfer on condition that all necessary supplementary measures are put in place. If some of these measures are not already in place (4B), you must proceed to step 5.

If you conclude that it is not possible to implement the necessary supplementary measures to ensure the effectiveness of the transfer tool, **you should not proceed with the planned transfer or you should cease any ongoing transfer**. In this case, the personal data that has been transferred must be returned, or deleted in its entirety.

DRAFT

Step 5 – Implement the Supplementary Measures and Take Procedural Steps Necessary

Once you have identified the appropriate supplementary measures to ensure that the data transferred enjoys a substantially equivalent level of protection as the one provided for under EU law, you can list in the table below the actions to be taken in order to implement the supplementary measures that must be implemented and in order to respect any procedural steps that must be followed.

The procedural steps you will have to follow may vary depending on the transfer tool in place . The EDPB recommendations on supplementary measures list some of these formalities.

Step 5: Implementation of the Supplementary Measures	
Action 1 *Name:*	*Describe the action:*
	Person in charge:
	Scheduled completion date:
Action 2 *Name:*	*Describe the action:*
	Person in charge:
	Scheduled completion date:
…	…

Opinions
Opinion of the Person in Charge of Data Protection (or of the Data Protection Officer, if applicable)
Opinion of the Person in Charge of Information System Security (or of the Chief Information Security Officer, if applicable)

Validation ***By the Person Responsible for the Transfer in Accordance with Internal Governance Rules***

DRAFT

Step 6 - Re-evaluate at Appropriate Intervals

It is necessary to reassess at appropriate intervals the transfer tool and, if applicable, the supplementary measures used for your transfer. This is essential to ensure that you suspend or cease your transfers promptly if the transfer tool or supplementary measures are no longer effective in the third country. To this end, you can set up a periodic review of your transfers in the table below.

In various circumstances, it may be necessary to reassess the protection of your 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 EU institutions' assessment of the law applicable in the third country.

Step 6 - Re-evaluate at Appropriate Intervals	
Intervals Between the Reviews	
Date of the Next Review	
Anticipated Review, Where Applicable, And Justification for Anticipation	

DRAFT