Public consultation on the practical guide

“Tranfer Impact Assessment”

Summary of contributions

January 2025

From December 2023 to February 2024, the CNIL put out to public consultation its practical guide on conducting Transfer Impact Assessments (TIA).

The contributions received helped to enrich the work on the final version of the guide.

This summary presents the main remarks received and the CNIL's response to them.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Summary of contributions on the practical guide “Tranfer Impact Assessment”

This public consultation received contributions, mainly from professionals in the sector (data protection officers, lawyers, consultants, heads of professional networks) concerned by the subject of transfers. The CNIL provides a summary of the contributions here.

About the CNIL's public consultation on its draft TIA Guide

A very large number of data controllers and processors are concerned by the issue of transfers. In its so-called ‘Schrems II’ judgment, the Court of Justice of the European Union (CJEU) emphasised the responsibility of data exporters and importers to ensure that personal data is processed, and continues to be processed, in compliance with the level of protection set by European Union data protection legislation. Accordingly, exporters relying on the transfer tools listed in Article 46 of the GDPR for their personal data transfers are obliged to assess the level of protection in third countries of destination and the need to put in place additional safeguards. Such an assessment is commonly known as a Transfer Impact Assessment (TIA).

In line with the Recommendations of the European Data Protection Board (EDPB) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, the CNIL drew up a Guide for exporters to help them carry out their TIA.

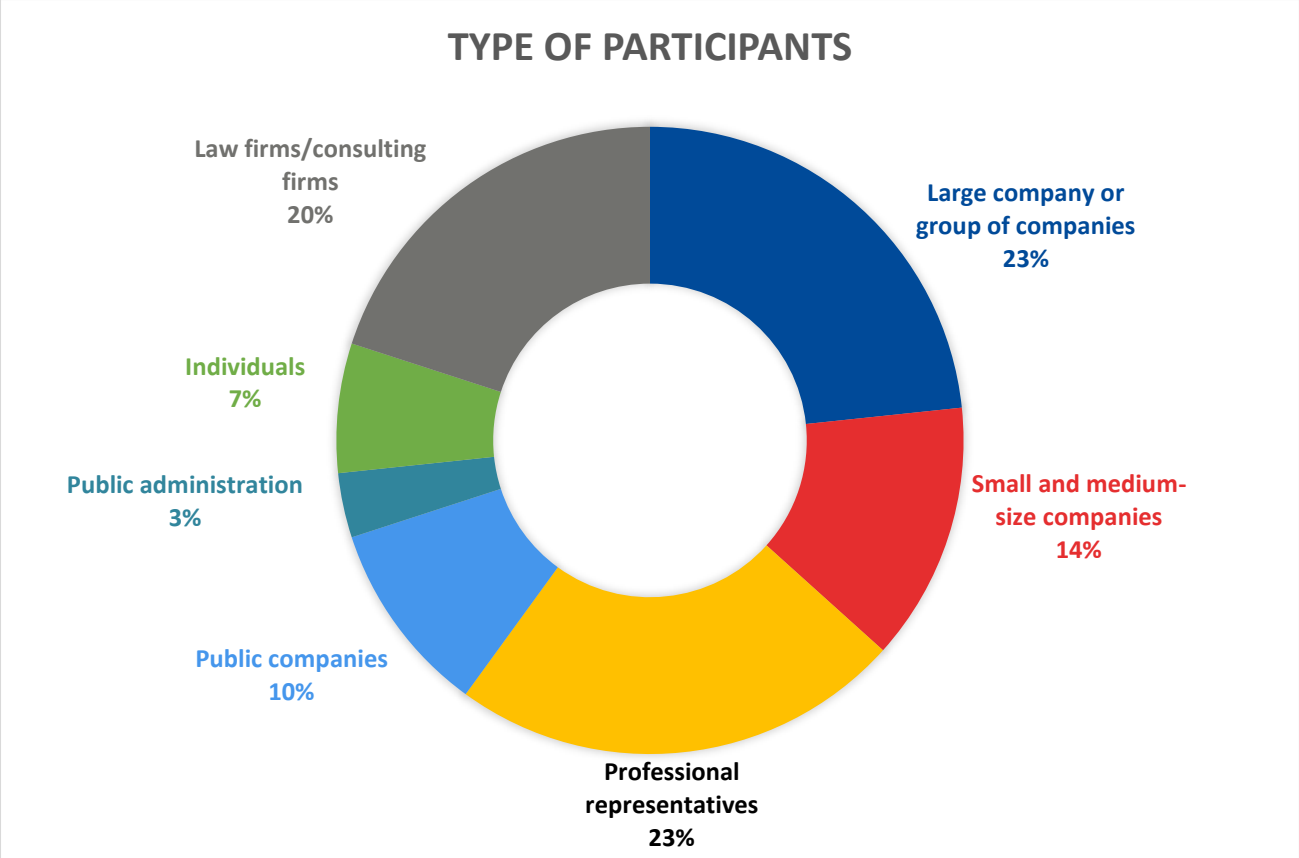
The TIA guide is a methodology which identifies the stages prior to carrying out a TIA and the various elements to be taken into account when carrying out a TIA. It gives indications on how the analysis can be carried out by following the six steps set out in the EDPB Recommendations, and refers to the relevant documentation. It does not constitute an assessment of the laws and practices of third countries, and the associated risks. Its use is not compulsory; other elements may also be taken into account and other methodologies applied.

The draft Guide was the subject of a public consultation between December 2023 and February 2024, in preparation for its final version.

Key figures

The consultation received 34 contributions, mainly from professionals in the sector (data protection officers, lawyers, consultants, heads of professional networks). The contributors represent actors of all sizes (French and international groups, small and medium-sized enterprises, professional networks/business federations, etc.) and of a variety of sectors (banking/finance, insurance, transport, industry, digital/IT, cosmetics/health, local and regional government, etc.).

- 75% of those taking part in the consultation are experts (data protection officers, lawyers or data protection consultants)
- 23% of participants are representatives of professional associations
- 23% of participants are representatives of large companies



All these contributions enabled the CNIL to improve the form and content of its Guide in order to clarify and specify its content; and to consolidate or adjust certain ideas and analyses, in particular to take account of the latest opinions of the European Data Protection Board.

Main remarks received and the CNIL's responses

Below is a summary of the main comments we received and processed. A large number of proposed amendments were incorporated into the final version of the Guide, but are not analysed here because they do not raise any structural points of the Guide.

On the difficulties encountered by small and medium-sized players in carrying out TIAs

Remark: Several organisations shared their regret that the Guide provides for the same approach regardless of the size of the organisation; that small and medium-sized enterprises, craftsmen or the liberal professions are treated in the same way as multinational companies. Others, even large ones, mentioned the great difficulty faced by European companies and administrations in analysing the legal framework and practices in third countries.

Response CNIL: The GDPR provides for a uniform approach regardless of the size of the players involved. The CJEU, which introduced the data transfer impact assessment exercise, and the European Data Protection Board (EDPB), which provided a methodology through its Recommendations 01/2020, provide for a uniform approach regardless of the size of the organisation. That said, the degree of checks carried out in a TIA will depend on the resources available to the exporter and the assistance provided by the importer.

This guide contains a proposed methodology for conducting a full TIA, including some optional sections, with information that may help the exporter in its assessment.

The guide is organised around the 6 steps recommended by the EDPB: 1) Know your transfer; 2) Identify the transfer tool used; 3) Assess the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool; 4) Identify and adopt supplementary measures; 5) Implement the supplementary measures and any procedural steps and 6) Reassess at regular intervals. The description of the transfer (in step 1) enables, in particular, to take into account its characteristics and sensitivity when assessing the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool (in step 3) and when assessing the additional measures to be put in place (in step 4).

We are also aware of the difficulties faced by small and medium-sized organisations, particularly when assessing the legislation and practices of third countries. When acting as exporters, we encourage them to seek the assistance of the data importer and to ask him to provide any useful information enabling the exporter to carry out an analysis of local legislation and the practices of public authorities in terms of access (see also the following question). We also invite them to draw on existing analyses such as the page 'Data protection around the world' on the CNIL website, as well as reports by reputable international organisations, and expert analyses such as those commissioned by the EDPB for certain countries (Russia, India, China, Brazil, Mexico, Turkey). Finally, we invite them to share their analyses through professional associations, networks of data protection officers, and groups of companies or administrations.

On responsibility for carrying out the TIA

Remark: Most organisations raised the question of which entity in a processing chain is responsible for carrying out a TIA. Several mentioned the lack of active cooperation by the importer as the main obstacle to carrying out the TIA, given the difficulty and high cost associated with assessing the third country's legislation and practices.

Response CNIL: The question of responsibility for carrying out the TIA depends on the role of the parties involved in the transfer (exporter/importer) and in the processing (controller/processor). We included 3 scenarios to address the most common cases encountered in practice. These scenarios are in line with EDPB Opinion 22/2024 on the responsibility of controllers in a long chain of subcontracting.

In principle, the TIA must be carried out by the exporter, whether acting as controller or processor, with the assistance of the importer.

> **Case 1 - Controller in the EEA acting as an exporter transferring data to a processor acting as an importer in a third country:**
>
> In this case, the controller is obliged to carry out the TIA with the collaboration of the processor.

Case 2 - Processor in the EEA acting as exporter transferring data to a subsequent processor acting as importer in a third country:

In this case, it is the processor's responsibility to ensure that its transfer is compliant and to carry out the TIA. Pursuant to Article 28(3)(h) of the GDPR, the processor is required to provide the controller with information to demonstrate compliance with its obligations, including the TIA carried out. Pursuant to Article 28(1) of the RGPD, the controller is required to verify the guarantees offered by the exporting processor. The controller may rely on the information received from the processor, including the TIA.

Case 3: Controller in the EEA acting as an exporter transferring data to a data controller in a third country:

In this case, the controller-exporter is required to carry out the DTIA with the collaboration of the controller-importer.

On the definition of the notion of transfer

Remark: Several organisations requested that the Guide define the concept of transfer, as well as the concepts of importer and exporter of data, citing examples of transfers. The organisations raised several complex cases: (i) the case of transfers from a controller to a processor in the EEA who subsequently transmits the data back to the same or another third country; (ii) the case of intra-group transfers; (iii) the case of employees teleworking from third countries and (iv) the case of direct collection of data by a controller in a third country.

Response CNIL: We made the choice of referring to the work of the European Data Protection Board (EDPB), which drew up definitions in its 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. In addition to the definitions, these Guidelines contain 11 examples that clarify the most common cases of data transfers. The CNIL will also be publishing a General Guide on Data Transfers in the coming months.

On the scope of the TIA

Remark: A significant number of organisations raised the question of how far the obligation to carry out a TIA extends in the context of a long chain of processing. Several mentioned the fact that data controllers do not have the means to carry out a TIA for each subsequent transfer of data envisaged by each of their service providers.

Response CNIL: We added a new section to the Guide (2.4) which answers this question. In its Opinion 22/2024, the EDPB specifies that the exporter's analysis must take into account the entire life cycle of the data, including subsequent transfers, so that the controller (whether or not it is the exporter itself) can assess the risks associated with all data transfers outside the EU.

A TIA may concern a single transfer or a series of transfers. The exporter therefore has the choice of documenting their analysis in the same document or in several documents. If there is a change in the transfer chain, the exporter can link their new analysis to the pre-existing analyses already carried out. If the exporter is a processor, they must share this information with the controller.

On the description of the transfer (step 3.1)

Remark: Several organisations made suggestions for rewording the sections in this part of the Guide.

Response CNIL: We accepted the vast majority of these proposals. The new section is simpler in some respects (e.g. deletion of the 'nature of the exporter's activities') and more precise in others (e.g. addition of examples of the method of transfer, addition of a list of categories of data transferred). We chose not to specify certain elements despite requests, such as the categories of data subjects, as this can change from one organisation to another. Other information was added, but remains optional: total or partial nature of the transfer, volume of data and number of data subjects.

On the choice of the transfer tool (step 3.2)

Remark: Several organisations pointed out that the choice of tool comes before the TIA is carried out, since the latter is not compulsory in the case of a transfer to an adequate country or in the case of use of Article 49 derogations.

Response CNIL: We simplified this section, which now only lists the transfer tools set out in Article 46 GDPR. The elements relating to adequacy and derogations are developed in the introductory section 2.2. and will be the subject of subsequent work (see above on a general guide on transfers).

On the assessment of the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool (step 3.3)

Remark: Several organisations informed the CNIL that they face big difficulties in assessing the legislation and practices of the country of destination of the data. These difficulties begin with the collection of information and the reliability of information, and continue when it comes to monitoring changes in the legislation and practice of the destination country. Analysing the rule of law in third countries is particularly complex and costly, requiring in-depth knowledge of local law and practices. While some large companies may have competent in-house legal departments, this is not the case for artisans, self-employed professionals and small or medium-sized businesses. As the subject is complex and depends on the country, even companies with a competent in-house legal department are likely to have to call on specialist external advice.

Moreover, some point out that the notion of 'rule of law problem' is unclear in that it does not refer to precise legal criteria.

Others invite us to take a position on these issues, which would be common to all exporters, or ask for this analysis to be carried out at EEA level. They invite the CNIL or the EDPB to make available to these exporters a repository of legislation and practices applicable to countries not covered by an adequacy decision.

Some add that the assessment of national legislation involves political and economic issues that go beyond the simple contractual relationship between an exporter and an importer of data.

Lastly, several organisations mention the subjective nature of the assessment and the risk of fragmentation in the application of Chapter V of the RGPD.

Response CNIL: We are aware of the difficulties linked to the analysis of the legislation and practices of third countries. To answer as much as possible to these problems, we have modified step 3.3 of the Guide in order to emphasise (i) the need for collaboration on the part of the importer of the data, who is supposed to know the local legislation and the practices of the competent authorities in their country, or at least who is in a better position to obtain this information; (ii) the resources on which exporters can rely to carry out their assessment.

These resources include the page 'Data protection around the world' on the CNIL website (regularly updated), reports from reputable international organisations and expert analyses such as those commissioned by the EDPS for certain countries (Russia, India, China, Brazil, Mexico, Turkey). We also invite exporters to share their analyses through professional associations, networks of data protection officers, and groups of companies or administrations.

Generally speaking, the CNIL is not responsible for analysing the legislation and practices of third countries. Such an analysis is carried out by the European Commission in its adequacy decisions in accordance with Article 45 of the RGPD, but it is not the responsibility of the national data protection authorities to carry out such an assessment. Furthermore, this analysis cannot be dissociated from the analysis of the specific conditions of each transfer and the particularities of the processing that only the exporter and importer have control over.

On assessing the independence of third country data protection authorities (step 3.3)

Remark: Some organisations mention their difficulty in analysing the degree of independence of data protection authorities in third countries and invite the CNIL to provide an assessment of the degree of independence of the various data protection authorities or, at the very least, to specify criteria for evaluating the independence of the authority.

Response CNIL: As with the analysis of legislation and practices in third countries, it is not within the CNIL's competence to assess the degree of independence of the various data protection authorities around the world. To help exporters in their assessment, we have added a few elements that they may take into account: articles 52 to 54 of the GDPR; article 15 of the Council of Europe's Convention 108+; the works of the Global Privacy Assembly (GPA); the more general works of the Organisation for Economic Cooperation and Development (OECD).

On the proof that the authorities of the third country have no access to the data transferred (step 3.3)

Remark: Some organisations cite the difficulty in demonstrating that the importer has not received a request for access to EU data subjects' data or that the importer has been subject to direct access by the authorities of the third country.

Response CNIL: We added that exporters may rely on the importer's transparency report on access requests by the authorities and we have limited the verification in time by indicating that the importer must demonstrate that, at least over the last few years, they have not received an access request or been subject to direct access by the authorities of the third country.

In accordance with EDPB Recommendations 01/2020 (§43.3), we have also provided for cases where, despite the fact that the transfer tool is not effective in the light of the assessment carried out, the exporter has no reason to believe that the problematic legislation will be applied in practice to the transferred data, and thus may decide to proceed with the transfer without implementing supplementary measures. In these exceptional cases, the exporter will have to demonstrate and document this assessment, where appropriate in collaboration with the importer and also taking into account the experience of other players operating in the same sector and/or in sectors linked to similar transfers.

On the assessment of existing and supplementary measures (stage 3.4)

Remark: Some organisations asked the CNIL for guidance on the approach and methodology to be adopted when assessing existing and supplementary measures and for the CNIL to provide examples.

Response CNIL: We specified in a footnote the points of control that exporters must check with the help of importers in order to ensure that the security measures are effective in preventing access to the data by the authorities of third countries. These points of control are based on the use cases developed by the EDPB in its Recommendations 01/2020.

On the sufficiency of contractual and organisational measures (step 3.4)

Remark: Several organisations noted that the initial version of the Guide was stricter than EDPB Recommendation 01/2020 in that it stated that '*contractual and organisational measures are not in themselves sufficient to prevent possible access to data by the authorities of the third country and must be supplemented by technical measures*'.

Response CNIL: We aligned the wording of our Guide with Recommendations 01/2020. In any event, according to these Recommendations: "*Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices. Indeed there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes. In such situations, contractual or organisational measures may complement technical measures and strengthen the overall level of protection of data (e.g. by introducing checks and eliminating automatisms for attempts from public authorities to access data in a manner not compliant with EU standards).*"

On the implementation of supplementary measures (stage 3.4)

Remark: Some organisations cited the difficulty of implementing these measures, particularly for self-employed professionals and small and medium-sized businesses.

For larger players, the benefits of compliance in relation to business needs sometimes do not justify spending time on this exercise. The security measures proposed by the EDPB and included in the Guide are not adapted to a large number of services, in particular cloud data hosting and the provision of technical resources (SQL queries, HPC, etc.), which makes it impossible to ensure compliance for these data transfers.

Response CNIL: The very purpose of the TIA is to enable the exporter to identify measures that would prevent access to transferred data by third-country authorities operating within a legal framework that does not provide appropriate safeguards for the rights and freedoms of data subjects. In cases where no security measures are

suitable for the processing envisaged, or where the implementation of the envisaged measures is too costly, data controllers or processors must refrain from the envisaged transfer.

On the termination of transfer in the event of non-compliance (step 3.4)

Remark: When the TIA leads to the conclusion that it is not possible to put in place the necessary measures to ensure the effectiveness of the transfer tool, but the transfer is already underway, some organizations have suggested adopting a risk-based approach by immediately ceasing the transfer only when the processing presents high risks to the rights and freedoms of the data subjects. In the opposite case, i.e. in the absence of such a high risk, some organizations have suggested stopping the transfer only when the contract comes to an end, or when a certain period expires.

More generally, several organizations pointed to the considerable impact that a suspension of transfer can have, given the current business model of many companies that host their data with providers outside the EU.

Response CNIL: The very purpose of the TIA is to enable the exporter to identify measures that would make it possible to prevent access to transferred data by third-country authorities operating within a legal framework that does not provide appropriate safeguards for the rights and freedoms of data subjects. Where this is not possible, the controller or processor must refrain from the transfer, or stop it if it is already underway. The conditions for implementing the transfer termination order must then be determined on a case-by-case basis.

On re-evaluating the analysis at appropriate intervals (step 3.6)

Remark: A number of players pointed out the difficulties of regularly analysing the laws and practices of third countries. In their view, they cannot be aware of all legislative changes, and are less well placed than French and European public authorities to carry out this monitoring and assessment exercise, which can be carried out at institutional level within the framework of inter-state relations.

Response CNIL: We are aware of the difficulties organisations face in anticipating such changes. It is advisable to keep a close eye on the latest legislative developments on data protection in all the countries to which the exporter transfers data, so as to be better able to anticipate whether the reassessment of data protection in that country proves necessary. In any case, these appropriate intervals are to be determined by the exporter 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.