May 2023

EU: EDPB's finalized guidelines on international data transfers under the GDPR explained

On February 24, 2023, the European Data Protection Board (EDPB) published its finalized 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. A draft version of the Guidelines - which aim to clarify the interaction between Article 3 of the General Data Protection Regulation (GDPR) and Chapter V of the GDPR - was released for public consultation in November 2021.

Wim Nauwelaerts, Partner at Alston & Bird LLP, provided an overview of the draft Guidelines back in 2021. He now discusses the finalized Guidelines and their importance for transfers of personal data under the GDPR.

imaginima / Signature collection / istockphoto.com

The GDPR does not define what constitutes an 'international data transfer' (IDT) to a third country or to an international organization for purposes of Chapter V of the GDPR. The initial idea behind this omission was to provide supervisory authorities with a maximum degree of flexibility when monitoring companies' compliance with the GDPR. The EDPB, however, has now acknowledged that the lack of clarity around the concept of IDT has resulted in legal uncertainty and divergent approaches to compliance with, in particular, the data transfer restrictions in Chapter V of the GDPR. Therefore, the EDPB has created the Guidelines to clarify the scenarios to which it considers that the requirements of Chapter V should be applied. The Guidelines also include examples of data flows to third countries, which are illustrated in an annex with a view to providing further practical guidance.

Chapter V

Chapter V of the GDPR is aimed at ensuring the continued protection of personal data after it has been transferred to a country outside of the EU (or to an international organization). When personal data is transmitted or made available to a recipient outside of the EU (or to an international organization), there is always a risk that the level of protection of individuals' rights and freedoms may not be 'essentially equivalent' to the one afforded by the EU's legal framework. Continuity of protection can be achieved in different ways, including through the system of adequacy decisions (adopted by the European Commission) or by data transfer 'instruments' that the data exporter and importer have implemented and that provide for appropriate safeguards. According to the EDPB, the risk of discontinued protection does not only exist when personal data is transferred to a data importer whose processing is not in scope of the GDPR. Where a controller or processor transfers data to a data importer whose processing falls under Article 3(2) of the GDPR, the protection provided by the GDPR may similarly be undermined by the legal framework that applies to the importer.

The Guidelines' objective is to clarify this interplay between Article 3 of the GDPR and the provisions on IDTs in Chapter V of the GDPR. The purpose is to assist controllers and processors with identifying whether a processing operation constitutes an IDT and whether they have to comply with the provisions of Chapter V of the GDPR. The EDPB considers that this clarification is also important for the consistent interpretation and application of the GDPR by the supervisory authorities. In addition, the Guidelines intend to highlight that even when a certain data flow does not constitute an IDT under Chapter V, the processing of personal data outside of the EU can still trigger increased risks for individuals. In that case, it may be necessary to envisage putting in place appropriate safeguards.

Criteria-based approach

To clarify the scenarios to which the transfer restrictions of Chapter V apply, the EDPB has identified three cumulative criteria that must be met for a processing operation to qualify as an IDT:

- there is a data exporter, which is a controller or a processor subject to the GDPR for a given processing activity;
- that exporter discloses by transmission or otherwise makes personal data, subject to the processing, available to another controller, joint controller, or processor (i.e., the importer); and
- the importer is located outside of the EU - irrespective of whether or not this importer's processing is subject to the GDPR - or is an international organization.

First criterion

As a preliminary condition, there can only be an IDT if there is a controller or processor that is subject to the GDPR for a specific processing activity, in accordance with Article 3 of the GDPR. Often that controller or processor will be established in an EU Member State, but pursuant to Article 3(2) of the GDPR controllers and processors without an establishment in the EU may also be subject to the GDPR for a given processing. Those 'non-EU' controllers and processors will also have to comply with the transfer restrictions in Chapter V of the GDPR.

Second criterion

The second criterion requires that the data 'exporter' discloses personal data by transmission or otherwise makes personal data available to another (joint) controller or processor. The concept of making personal data available appears to be very broad in the eyes of the EDPB, and includes remote access from outside of the EU - even if it takes place only by means of displaying personal data on a screen, for example, for IT support/troubleshooting purposes.

Referencing to previous guidance on the concepts of controller and processor under the GDPR, the EDPB further emphasizes that a case-by-case analysis of the processing at stake and the roles of the actors involved may be necessary to determine whether the second criterion is met. The EDPB also clarifies that the second criterion is not met in the following cases:

Internal processing

Internal processing covers transmissions of personal data within the same controller or processor, even if the processing takes place outside of the EU.

Example

The Guidelines provide the example of an employee of an EU-based company who travels to a country outside of the EU for a meeting bringing their laptop. During their stay abroad, the employee uses the laptop to remotely access the company's database containing personal data. This remote access of personal data from a third country does not qualify as an IDT, as the employee is not a separate controller. This is considered as a transmission that is carried out within the same controller (i.e., the EU-based company). However, if the employee - in the course of performing their job duties - would send or make data available to another controller or processor in the third country, the data flow in question would amount to an IDT under Chapter V of the GDPR: from the employee's company in the EU (the data exporter) to the data importing controller or processor in the third country.

Conversely, legal entities that form part of the same corporate group may qualify as separate controllers or processors. Therefore, a cross-border disclosure of personal data between entities belonging to the same corporate group could constitute an IDT under Chapter V of the GDPR.

Example

The Guidelines provide the example of a company in Ireland that is a subsidiary of a parent company outside of the EU. The Irish company discloses personal data relating to its employees to the parent company with the instructions to store it in a centralized HR database in the third country. In this case, the Irish company discloses the personal data as an employer/controller to the parent company, which is acting as a processor. The Irish company is established in the EU and therefore subject to the GDPR, while the parent company is situated in a country outside of the EU. The disclosure qualifies as an IDT within the meaning of Chapter V of the GDPR.

Scenarios in which there is no controller or processor acting as a data exporter

This scenario applies, for instance, when an individual in the EU sends its personal data directly to a recipient outside of the EU.

Example

The Guidelines provide the example of an individual in Italy that fills out an online form to purchase clothing on a website operated by a company that has no presence in the EU, but that specifically targets consumers in the EU. In that case, the individual shares its personal data directly with the company outside of the EU. This does not constitute an IDT, as the data is not disclosed by an exporter (controller or processor), but by the individual directly. Nonetheless, the company outside of the EU will be required to comply with the GDPR since its processing operations are subject to Article 3(2) of the GDPR (targeting of individuals in the EU by offering them goods).

An IDT may not only be carried out by a controller, but also by a processor. There may be an IDT where a processor (either under Article 3(1) or 3(2) of the GDPR) discloses personal data to another processor or even to a controller outside of the EU.

Example

The Guidelines provide the example of a controller in the US (without an EU establishment), which sends personal data of its employees/customers - all of the individuals not located in the EU - to a processor in the EU. The processor subsequently re-transmits the data to the controller. The processing performed by the processor is covered by the GDPR for processor-specific obligations pursuant to Article 3(1), as the processor is established in the EU. Considering that the controller is in a third country, the EDPB takes the position that the disclosure of data from the processor (back) to the controller is an IDT. Interestingly, the same scenario would not be viewed as a 'restricted data transfer' under the UK General Data Protection Regulation (UK GDPR), if the processor were located in the UK instead of an EU Member State.

Third criterion

As a third criterion for an IDT, the data importer must be:

- located in a third country (i.e., outside of the EU), regardless of whether the importer's processing is subject to the GDP; or
- an international organization.

The Guidelines address the specific situation in which a controller in the EU uses a processor in the EU subject to third-country legislation. In that scenario, there is a possibility that the processor may receive government access requests triggering a transfer of personal data (if the processor acts on such a request). The EDPB recalls that under the GDPR, controllers may only use processors that provide sufficient guarantees in terms of technical and organizational measures to safeguard the controller's data. The GDPR does not only refer to expertise and resources, but also to reliability, which according to the EDPB may be in doubt if the processor is subject to third-country legislation (which may prevent it from fulfilling its obligations as a processor).

Example

The Guidelines provide the example of a controller in Denmark that engages a processor established in the EU, which is a subsidiary of a non-EU parent company. The processor processes personal data of the controller exclusively in the EU, and the processor's parent company outside of the EU has no access to the data. The processor is, however, subject to third-country legislation with extraterritorial effect, which means that it may receive access requests from foreign authorities. In this situation, the controller should, before engaging the processor, assess the access risk in order to ensure that, as required by Article 28 of the GDPR, it uses a processor that provides sufficient guarantees in line with the GDPR, including Chapter V. Should the processor comply with such foreign requests, the disclosure of personal data would be considered an IDT under Chapter V of the GDPR. If the processor complies with a request in violation of the controller's instructions, the processor shall be considered an independent controller of that processing under Article 28 of the GDPR. In that case, the initial controller in Denmark cannot be held responsible for the IDT.

Consequences of an IDT

If the three criteria for an IDT are met, the data exporter must comply with the conditions of Chapter V and justify (or, as the EDPB calls it, 'frame') the transfer by using one of the transfer instruments that aim at protecting personal data after it has been transferred outside of the EU or to an international organization.

The main types of transfer instruments listed in Article 46 of the GDPR are Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), codes of conduct, certification mechanisms, and *ad hoc* contracts. In exceptional circumstances, Article 49 of the GDPR makes it possible to transfer personal data to a third country or an international organization without the existence of an adequate level of protection or the implementation of appropriate safeguards, if one of the limited 'derogations' listed in Article 49 applies.

The Guidelines underline that the content of the safeguards offered by these transfer instruments must be adapted depending on the situation. For example, in the case of an IDT to a controller or processor outside of the EU that is already subject to the GDPR for a certain processing activity, the GDPR applies in its entirety to that processing. In this scenario, the EDPB is of the view that transfer instruments (such as SCCs) should not duplicate the GDPR obligations, but rather address the elements that are related specifically to the risks associated with the importer being located outside of the EU. This may include addressing possible national laws that allow for government access to data, as well as issues around redress possibilities against entities outside of the EU. It should also be noted that the European Commission has indicated that it is in the process of developing an additional set of SCCs for this scenario (which will complement the existing SCCs). However, the Guidelines remain silent on whether the existing SCCs can be used to 'frame' an IDT to a controller or processor outside of the EU whose processing falls in scope of the GDPR, as long as the European Commission has not issued an additional set of SCCs for this specific transfer scenario.

Processing outside of the EU without an IDT

The Guidelines recognize that there may be situations in which personal data is processed outside of the EU without there being an IDT. A data transmission may not qualify as a transfer to a third country in accordance with Chapter V of the GDPR, e.g., where an employee of an EU controller travels abroad and has access to the data of that controller while being in a third country. In those situations, the controller must still comply with the GDPR, and will remain accountable for the processing activities, regardless of where they take place. This also means that controllers (and processors) should pay particular attention to the legal frameworks of countries outside of the EU that may have an impact on their ability to respect the GDPR, for instance, in relation to disproportionate government access by third-country authorities. In some cases, controllers may be compelled to conclude that the processing abroad requires extensive security measures, or even that it would not be lawful to conduct or proceed with the processing operation, even if there is no IDT. When a controller intends to process personal data outside of the EU (although no international data transfer takes place), the EDPB recommends that the controller informs individuals accordingly, as part of the controller's transparency obligations under the GDPR.

Data processing in third countries can involve increased risks for individuals and their personal data, which according to the EDPB, must be identified and attentively addressed in order for the processing to be lawful under the GDPR. The EDPB has indicated that it will assess the need for additional guidance in this context, particularly on safeguards.

Wim Nauwelaerts Partner
wim.nauwelaerts@alston.com
Alston & Bird LLP, Brussels