Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

CEDPO comments on 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

The GDPR does not provide a definition of what is to be understood by a 'data transfer' according to Art. 44. This leads to legal uncertainties for controllers and processors especially when entering into agreements with multinationals. CEDPO therefore welcomes the EDPB's initiative to seek clarity in the field of international data transfers under the GDPR.

The EDPB has identified *three cumulative criteria* which need to apply in order to qualify a processing of personal data as data transfer.

1. A controller or processor is subject to the GDPR for the given processing

In order to ensure that the level of protection of natural persons by the GDPR is not undermined, a processing by a controller or processor needs to be subject to the Regulation in the first place. CEDPO fully agrees that this has to represent the first criterion when assessing a processing in an international context.

Considering the recognition by the GDPR that data transfers can be determined by data processors, CEDPO would welcome clarification on the responsibilities over data transfer

requirements between controllers and processors. In particular, when a controller purchases an application or the services of an EU processor, the controller often does not master nor has leeway over the data transfers operated behind the scene, especially in cloud environments.

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

- **International transfers are part of a broader concept.** A transfer of personal data can occur in various ways and by various means. This is why the notion of 'making available' is important to make controllers or processors aware that *access* to personal data by a third party can be sufficient to consider a processing a 'transfer'. Since the international data transfer is part of the broader concept of "data processing" according to Art. 4(2) GDPR, Guidelines 05/2021 should include references to WP29/EDPB Guidance on data processing and data transfers respectively.
  CEDPO would also welcome a clarification that the following situation does not constitute international data transfers per se:
    - Transferring data to a controller or processor located in the EU with controlled ownership by an entity located in a third country where the law permits access to data by public authorities;

  Furthermore, it should be explained whether the *intention* to make a transfer has to be taken into account when assessing the notion of a 'data transfer'. Especially in circumstances, where a controller in the EU receives an access request by a public authority from a third country, one could argue that a transfer does not take place since the controller does not determine the purposes and means of the processing, therefore is *lacking intention* to transfer personal data.

- **Interplay with ePrivacy.** While the GDPR (at least) offers a definition of a data processing, the notion of an 'international data transfer' requires further guidance when using electronic communications networks to store information or to gain access to information stored in the terminal equipment under the ePrivacy-Directive. CEDPO would therefore welcome if

the EDPB could elaborate on the interplay between the GDPR and ePrivacy-Directive regarding the definition of a data transfer to third countries.

- **The data subject's own initiative.** When personal data is disclosed directly by the data subject and on his/her own initiative, the EDPB does not consider the processing a transfer by a controller or processor. The application of the three cumulative criteria of a data transfer to this example would provide further clarity for privacy professionals including the DPO. Already in view of the first criterion 'controller or processor subject to the GDPR', the data subject him/herself cannot be controller or processor for his/her own personal data. This is the main reason why an international data transfer does not take place.

  In the employment context though it remains unclear, under which circumstances an employee processes personal data on his/her own initiative or, alternatively, on the instructions of the employer, requiring him/her to use a service which includes the transfer of personal data to another recipient. CEDPO therefore would welcome another example by the EDPB reflecting on the usage of employee self-service tools.

- **Personal data transfers by EU processors.** *Example 3* raises doubt whether Chapter V shall apply for the transfer of non-EU personal data by a processor in the EU to a controller in a third country. A processor with an establishment in the Union is subject to GDPR requirements. However, all GDPR requirements are not applicable to this data processing activity. Only those requirements which are relevant to the data processor activity in the EU should apply. Thus, the requirements for processors in view of Art. 3(1) such as data security (Art. 32 GDPR) are applicable. In the given example, the controller is not subject to the GDPR and the personal data does not relate to EU residents. Hence, imposing Chapter V requirements on the data transfer to the third country seems disproportionate. It imposes on the data controller (importer) to put in place safeguards essentially equivalent to those in the EU for personal data of data subjects which would otherwise have fallen under the laws of his own jurisdiction, had the controller used a processor in his own country. It also imposes on the data processor to perform a *transfer impact assessment (TIA)* to send data back to the country where it comes from, requiring the EU processor to challenge the laws and practices of the country where his client has chosen to establish his activities, hire his employees and makes his business. As a consequence, a data processor could be led, applying the EDPB guidance, if the TIA is negative, **to refuse to return to his client the data which he received from him after having processed it**. **This will**

endanger the client/supplier relationship and seems excessive considering that the compass should be the data subject rights and freedoms: the transfer back will not create a particular additional risk for the data subjects, since without the processor intervention, it would have been processed by the data controller in the third country.

- **Onward transfers.** The involvement of two different (separate) parties should not systematically lead to the assumption of a transfer according to Chapter V. For instance, in the case that a data recipient in a third country relies on *contract workers* for certain processing activities, it remains unclear whether such involvement qualifies as an *onward data transfer*. Contract workers usually are independent workers or from a different legal entity but on a practical standpoint they are fully integrated in the data importer's infrastructure, including his technical and organisational measures, acting upon his/her instructions.

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

- **GDPR applicability cannot change locality of data.** Being subject to the GDPR concerning the respective data transfer does not change the location of establishment of the data importer in a third country. Consequently, a transfer takes place to any data recipient in a third country regardless of the applicability of the GDPR to him, existing adequacy decisions by the Commission or other appropriate safeguards. Nonetheless, the question remains, why a transfer of personal data would need appropriate safeguards under Chapter V when the GDPR itself is applicable for the processing and therefore is offering protection for the rights and interests of the data subject. The scope of application and content of such safeguards would possibly be very limited.

- **Complexity of GDPR assessments.** Under Example 7 it is specified that the data controller in the third country who resorts to an EU processor is subject to the GDPR. It would be beneficial to provide other examples to illustrate this case or to provide more precisions about it. For example, it is unclear whether the re-transmission of personal data by the EU

processor includes personal data of EU residents or data of third country data subjects. Instead of transferring the data to the third country controller, the EU processor might as well transfer the data to another processor in the third country which raises the questions of the applicable safeguard. Besides, Example 7 reveals that sophisticated legal analysis will be required on the data exporter and data importer's side to assess whether the GDPR is applicable. Depending on the result, the question of appropriate safeguards for the data transfer has to be dealt with additionally. Only few organisations will be able to perform such comprehensive analysis. Data protection is becoming more and more a legalistic exercise, drifting away from its original objectives: ensuring data subjects a transparent, secure, lawful processing of personal data.

31/01/2022

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu