Contribution to the public consultation on the 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

Laura Drechsler* and Svetlana Yakovleva**

1. Introduction

The **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** proposed for public consultation ('the Guidance') deal with a topic that has long puzzled the data protection community – the identification of international personal data transfers. The General Data Protection Regulation (GDPR) does not define international personal data transfers, though it requires their identification for the application of its transfer rules in Chapter V. It is therefore principally to be welcomed that the European Data Protection Board (EDPB) has tried to address the legal uncertainty stemming from the absence of a clear concept of international personal data transfer, especially in relation to the territorial scope of the GDPR regulated in Article 3.

However, as legal researchers active in this area,[1] we would nevertheless like to raise three areas to the attention of the EDPB that in our opinion are not sufficiently considered in the guidelines and should be addressed in the revised version after the public consultation. These are: i) the level of detail of the definition of 'data transfer' provided, ii) the potential inconsistency for the application of the GDPR by excluding from the definition of a transfer direct transmissions of personal data from an individual residing in the European Economic Area (EEA) to entities outside of it ('direct transmission from the data subjects'), and iii) measures to ensure the protection of individuals is not undermined when Chapter V is not applicable in the latter situation.

2. The level of detail of the definition

The definition provided by the EDPB in the Guidance is built on three cumulative criteria revolving around the actors involved in a processing operation. The definition however does not offer any details on which processing operations are to be considered as transfers exactly and whether the transferring of personal data requires any level of knowledge or intent as suggested by the definition of international personal data transfer in the Europol Regulation.[2] Granted the EDPB does state that transferring personal data is a disclosure of personal data 'by transmission'

* Laura Drechsler is a Ph.D researcher funded by the Flemish Research Fund (FWO personal mandate 1165319N) at the Law, Science, Technology and Society Research Group (LSTS) at the Vrije Universiteit Brussel (VUB).
** Svetlana Yakovleva, PhD, is a Postdoctoral researcher at the Institute for Information Law (IViR), University of Amsterdam and Senior Legal Adviser at De Brauw Blackstone Westbroek. The opinions expressed in this document are author's own and do not represent those of her employers.
The authors would like to thank Dr. Irene Kamara (Tilburg University) for her detailed feedback on an earlier draft.
[1] See also Laura Drechsler, 'Defining personal data transfers for the context of the General Data Protection Regulation', 10(1) *Privacy in Germany* (2022), pp. 24-29; Laura Drechsler and Irene Kamara, 'Essential Equivalence as a Benchmark for International Data Transfers After Schrems II', in Eleni Kosta and Ronald Leenes (eds.), *Research Handbook on EU data protection* (Edward Elgar Publishing Ltd., Forthcoming), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881875; Svetlana Yakovleva, 'GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives', *European Law Blog* (9 December 2021), available at https://europeanlawblog.eu/2021/12/09/gdpr-transfer-rules-vs-rules-on-territorial-scope-a-critical-reflection-on-recent-edpb-guidelines-from-both-eu-and-international-trade-law-perspectives/.
[2] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53, Art. 2(m).

or by 'otherwise' making personal data available.[3] This seems to suggest a very broad understanding of processing operations that could qualify as a transfer, which in turn would confer with the case law of the CJEU in *Schrems I* and *Schrems II* that views transferring personal data always as an act of processing personal data.[4] We would therefore suggest that should it have been the intention of the EDPB to state such a broad understanding, to make this more clear. Such an approach would in our opinion certainly be most consistent with CJEU case law and existing guidance of the EDPB.[5]

Regarding the question of knowledge or intent required for a transfer, it would be advisable that the EDPB clarifies whether this is a condition to qualify a processing operation as a data transfer. In our reading of the guidelines, the fact that such an element has not been mentioned might already signal that intention or prior knowledge is not required as a condition for a processing operation to qualify as a transfer according to the EDPB. This would align with the understanding that the GDPR in general is 'intent-agnostic'.[6] It also would complement the principle of accountability of controllers and processors for data transfers, that the EDPB has emphasized in its other guidance, and that requires a certain level of care of data exporters to ensure that they recognize and map all data transfers in the first place.[7] It also has to be noted however that the definition of transfers in the Europol Regulation suggests that an element of knowledge or intent is needed.[8] It would therefore be welcome if the EDPB would provide clarification on the effect of this definition and how it relates to the approach taken in the Guidance being discussed. Considering the use of the notion of data transfer also in the Law Enforcement Directive (LED), it would also be of use if the EDPB could note whether the same understanding as proposed in the Guidance also applies to the LED, of course adapted to its specificities (such as the absence of a provision similar to Article 3(2) GDPR).

3. Ensure consistent protection of personal data

The definition proposed by the EDPB excludes direct transmissions from the data subject from its understanding of a 'transfer' and thereby from the scope of application of Chapter V GDPR. Such an exclusion creates significant inconsistencies for the protection afforded to individuals through the GDPR, and those inconsistencies would warrant further clarification in the Guidance.

3.1 Inconsistency of the protection within the GDPR

Based on Article 3 GDPR and the Guidance, we discern the following four different situations of data flows, in each of which personal data is afforded *a different level of protection*.

1. Situation 1: Direct transmission of personal data from a data subject to a non-EEA entity that falls under the GDPR by virtue of Article 3(1) or 3(2) GDPR (for example, collection

[3] European Data Protection Board, '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' (Version for public consultation, 18 November 2021), p. 4, para. 7, indent 2.

[4] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650), para. 45; Case C-362/14, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559), para. 83.

[5] See further Drechsler and Kamara (n 1), pp. 5-7.

[6] Jef Ausloos, Michael Veale and René Mahieu, 'Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance', 10(3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2019), pp. 283-309, 296.

[7] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (Version 2.0, 18 June 2021), pp. 9-11.

[8] Art. 2(m) Europol Regulation (n 2) defines 'transfer of personal data' as 'the communication of personal data, actively made available, between a limited number of identified parties, **with the knowledge or intention of the sender** to give the recipient access to the personal data' (emphasis added).

of personal data by a foreign entity of an online shop that also has an establishment in the EEA or online tracking). In this situation, which does not qualify as a 'transfer' according to the Guidance, personal data is protected by the *GDPR rules except for the provisions of Chapter V*. Because the GDPR applies by virtue of its territorial scope provisions, interpretation of accountability, organisational and security obligations may compensate for the inapplicability of Chapter V (paras. 17, 24 of the Guidance).

2. Situation 2: Direct transmission of personal data from a data subject to a non-EEA entity, which does not fall under the scope of the GDPR, because the conditions of Article 3 are not met. In this situation, personal data processing is *not afforded any GDPR protection*. It should also be analysed whether this situation is purely hypothetical in the light of the broad scope of Article 3.
3. Situation 3: Transfer of personal data from an EEA exporter to a foreign data importer that falls under the GDPR by virtue of Article 3(1) GDPR. In this situation, personal data is protected by the *whole GDPR, including Chapter V*. This is likely to be the case in of personal data transfers between EEA and non-EEA establishments of multinational companies.
4. Situation 4: Transfer of personal data from an EEA exporter to a non-EEA data importer that does not fall under the scope of the GDPR by virtue of Article 3. In this situation, personal data is protected by *only Chapter V rules*.

In light of the aim of the GDPR, as clarified by the CJEU, to ensure 'effective and complete' protection of personal data[9], we find the rationale for different levels of protection in these situations unclear. This also leads to inconsistency of the GDPR's framework and may undermine the fundamental rights protection of the rights to personal data protection and privacy guaranteed by the EU Charter of Fundamental Rights. For example, in situation 1 the Guidance proposes to disapply Chapter V despite the fact that the GDPR applies to the non-EEA entity collecting data, while in situation 3 Chapter V does apply in addition to other GDPR rules. We believe that irrespective of the technicalities of a transfer, personal data should be afforded the same level of protection. From an enforcement perspective, basing the definition of 'transfer' on technicalities such as presence/absence of a data exporter, also adds an extra step of fact-finding (where the data flows from), which is often opaque and not readily visible to individuals or supervisory authorities. It also creates an incentive for multinational companies to reroute their transfers in a way excluding the application of Chapter V (shift from situation 3 to situation 1) to reduce their GDPR compliance burden.

From our perspective, the key stumbling stone in resolving this inconsistency is finding the right balance between the application of Article 3 GDPR and Chapter V, which is not an easy task. An important aspect in resolving this conundrum is ensuring a level playing field between EEA and third country entities collecting and processing personal data from the EEA. This requires, on the one hand, that non-EEA controllers and processors have the same GDPR compliance burden as their EEA counterparts (to ensure that EEA companies are not disadvantaged vis-a-vis their foreign competitors). On the other hand, that collection of personal data from outside the EEA in situations where the GDPR already applies, does not come with additional limitations. For example, applying Chapter V to direct transmissions of personal data in situations 1 and 2 would require non-EEA controllers/processors collecting personal data directly from individuals in the EEA to not only have a lawful ground for processing (Article 6 GDPR), but *also* a lawful ground

[9] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317), para. 34; Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, judgment of 5 June 2018 (Grand Chamber) (ECLI:EU:C:2018:388), para. 28; Case C-25/17, *Jehovan todistajat - uskonnollinnen yhdyskunta*, judgment of 10 July 2018 (Grand Chamber) (ECLI:EU:C:2018:551), paras. 66, 70.

for a data transfer under Chapter V as in this case two data processing operations (collection and transfer) would coincide. Thus, unlike EEA controllers/processors, their non-EEA counterparts will need two *different* lawful basis (one for each processing operation) instead of one. In other words, while an EEA controller/processor may collect personal data in the EEA on the basis of legitimate interest, a non-EEA controller/processor – for collection of the same data in the same situation – would, in addition, need a lawful ground for transferring data. Legitimate interest, however, is not mentioned as a lawful ground for transferring personal data in Chapter V GDPR. Such different treatment of EEA and non-EEA controllers/processors could lead to a violation of the EU's national treatment obligations under the General Agreement on Trade in Services).[10] At the same time, disapplying Chapter V in situations of direct transmission of personal data (as suggested in the Guidance) makes it harder to justify, from an international trade law perspective, that the application of the GDPR, including Chapter V, is necessary in situation 3.[11]

We also realize that exclusion of direct transmissions from the concept of 'transfer' could be because of limited applicability of appropriate safeguards under Article 46 GDPR to such transmissions (e.g., the SCCs, Codes of Conduct). We argue, however, that the scope of these safeguards as formulated in the GDPR has been narrowed down by interpretation. For example, codes of conduct seems to not apply to direct transmissions from individuals in the EEA to non-EEA controllers/processors on the basis of EDPB's own interpretation in draft Guidance.[12] The Standard Contractual Clauses have been repeatedly interpreted by the European Commission as applying to transfers between data exporters and data importers.[13] In sum, in our view, the issue of the relationship between Article 3 and Chapter V cannot be resolved by simply disapplying Chapter V in certain situations (such as direct transmission, situations 1 and 2), while applying it in similar other situations (situations 3 and 4). In contrast, it is necessary to analyse the level of protection afforded by the GDPR with and without Chapter V.[14] This analysis should allow to ensure, on a granular level of specific obligations for controllers/processors, equivalent level of personal data protection transferred outside the EEA in each of the situations.

3.2 Transfers and Article 3 GDPR

We would also like to raise to the EDPB's attention that a direct transmission of personal data can also occur in a situation where the receiving entity is in the scope of Article 3(1) GDPR. This is the case when a controller has an establishment in the EU, but the collection of personal data occurs directly from the data subject without involving said establishment.[15] We would like the EDPB to clarify whether such actions are also excluded from the scope of transfer in the understanding of the EDPB. This seems to be the case when reading the three criteria for transfers, however when it comes to the consequences discussed in section 3, the EPDB mentions the need

[10] For more details see Svetlana Yakovleva (n 1).
[11] Ibid.
[12] European Data Protection Board, 'Guidelines 04/2021 on codes of conduct as tools for transfers' (7 July 2021), para. 7, stating that 'It should also be noted that a code intended for transfers adhered by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporter) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controller/processors to adhere to such code themselves', which suggests that the Codes of Conduct, in the EDPB's view, are intended for transfers between data exporters and data exporters.
[13] See, e.g., Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ 2021 L 199/31, Clause 1(b).
[14] See also Christopher Kuner, 'Territorial Scope and Date Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection', *Legal Studies Research Paper Series University of Cambridge* (2021), pp. 22-23.
[15] For example, the transmission of personal data from Spanish search engine users to Google Inc. described in Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (n 9), para. 43.

for an extra set of SCCs only in the context of Article 3(2) and does not mention whether similar SCCs are necessary in case of direct transmissions in the context of Article 3(1).[16]

3.3 Protection for individuals via Article 3(2) GDPR

The exclusion of direct transmissions from the data subject also raises inconsistency issues when it comes to the protection provided for them. As noted in the EDPB Guidance the objective of the rules of Chapter V is 'to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data are transferred'.[17] It is at this point not completely clear whether the sole application of Article 3 GDPR would ensure that this level of protection is not undermined. As noted by Kuner, the whole of the GDPR was not designed to be applied directly by entities not territorially located in the EU.[18] There are therefore a number of questions on how in a case where only Article 3 GDPR applies the level of protection for individuals can be guaranteed, especially in terms of their data subject rights. Two issues seem thereby in urgent need of further clarification: transparency for individuals about personal data processing and enforcement of the GDPR via representatives. These issues have not been fully addressed in the Guidance provided for Article 3 GDPR.[19]

With regards to transparency, it has to be noted that Articles 13 and 14 GDPR include as one of the innovations of the GDPR a specific information obligation for controllers when it comes to international personal data transfers.[20] This information obligation should ensure that data subjects are aware that their data are being transferred and are given the tools to find out how the protection of their personal data and their rights is ensured. It is not clear whether in a situation of a direct transmission from the data subject to an entity outside of the EEA these information obligations would still apply, since in the understanding of the EDPB this would not constitute a transfer. From the perspective of the principle of transparency it seems paramount that the data subject is aware where their personal data are going regardless of whether a processing qualifies technically as a transfer in the understanding of the EDPB. It would therefore be welcome if the EDPB could specify which transparency obligations a controller has that is captured by Article 3 but whose dealings with EU data subjects might not qualify as a transfer.

In terms of enforcement, we note that it appears that the 'representative' of Article 27 GDPR was created to enabled enforcement of the GDPR against entities captured solely by Article 3(2) GDPR. We also acknowledge that the EDPB has already given guidance on the institution of a representative. We nevertheless believe that it would be essential for the EDPB to clarify some further aspects about the institution of a representative and how it can support the enforcement of data subject rights. We especially consider it important that the EDPB provides guidance on what should happen from the perspective of an individual complaint about personal data processing falling under the GDPR by virtue of Article 3(2) GDPR if the non-EEA entity being the subject of complaint did not appoint such a representative, even though it was legally required to do so.[21]

---

[16] EDPB 2021 (n 3), pp. 8-9.
[17] Ibid., p. 3. See also Art. 44 GDPR.
[18] Christopher Kuner 2021 (n 14), pp. 1-36, 25.
[19] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version 2.0' (12 November 2019), pp. 23-28.
[20] Arts. 13(1)(f) and 14(1)(f) GDPR.
[21] See further Thierry Zoller, 'How to effectively evade the GDPR and the reach of the DPA (CDPWE-0001) (Part 1)' (May 2020), available at https://blog.zoller.lu/2020/05/how-to-effectively-evade-gdpr-and-reach.html (accessed 3 December 2021). Listen further Serious Privacy, 'Quite Magical: All About NOYB (with Robert Romain), available at https://seriousprivacy.buzzsprout.com/840448/9201927-quite-magical-all-about-noyb-with-romain-robert (access 3 December 2021).

4. Conclusions

To conclude, we would like to request the EDPB to provide further clarification and guidance on the following points:

- Clarification on the scope of data transfers of the EDPB and the processing activities that are included in that scope.
- Clarification on whether the understanding of the concept of transfer of personal data, as proposed by the EDPB, requires that the transferring entity has any prior knowledge or intent for the data to be transferred.
- Clarification how the understanding of transfer of personal data, as included in the Guidance, relates to the definition of transfer in the Europol Regulation.
- Clarification on how the concept of transfer of personal data should be understood in the context of the LED.
- Reconsideration of whether the exclusion of direct transmissions (from the data subject to the entity in the third country) from the definition of transfer is coherent with the system of protection established by the GDPR.
- Clarification on the role of Article 3(1) in the definition proposed by the EDPB.
- Clarification on what transparency requirements apply and on the basis of which legal grounds in case personal data are directly disclosed by the data subject to an entity outside of the EU.
- Clarification on how the representative assists in the enforcement of data subject rights against entities captured by Article 3(2) GDPR, especially the consequences of not appointing a representative when required from the perspective of the individual.

We also want to highlight that we strongly believe that some of the issues raised in this contribution cannot be resolved by the powers vested in the EDPB. Instead it would be of importance for the legislator to step in order to resolve the issue of the relationship between Article 3 and Chapter V in a way ensuring equivalent protection of all personal data transmitted from the EEA, on the one hand, and a level playing field for EEA and non-EEA controllers/processors on the other hand.[22] To prepare such a legislative solutions, the EDPB could (with the help of experts) start developing a granular approach on the level of specific obligations of controllers/processors to resolving the relationship of Article 3 and Chapter V GDPR.

[22] For possible examples of how this conflict can be resolved by the legislator, see Christopher Kuner 2021 (n 14), pp. 33-35.