Comments on the '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'

Prof. Christopher Kuner
Brussels Privacy Hub and Vrije Universiteit Brussel (VUB)
Brussels, Belgium
January 2020

Introduction and scope of my comments

I am submitting these comments in response to the public consultation on the EDPB Guidelines 05/2021[1] (the 'Guidelines'). I am professor of law and co-chair of the Brussels Privacy Hub, a research centre in the faculty of law of the Vrije Universiteit Brussel (VUB). I am also a member of European Commission's Multisectoral Stakeholder Expert Group to Support the Application of the GDPR. Further information about me can be found on my website www.kuner.com.

These comments are made wholly in my personal capacity as an academic, and are based on the following two papers I have already published that go into this topic in greater detail:

Christopher Kuner, Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection, University of Cambridge Faculty of Law Research Paper No. 20/2021, 16 April 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850

Christopher Kuner, Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR, European Law Blog, 13 December 2021, https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr/

General Comments

I welcome the fact that the EDPB has decided to opine on the interplay of Article 3 and Chapter V, since clarity on the issues surrounding it is sorely needed. It is also commendable that the EDPB seems to recognize the need for a cumulative interpretation of the rules of Article 3 and Chapter V (see para. 3 of the Guidelines), i.e., that they are complementary and that one cannot be disapplied simply because the other applies.

[1] https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf.

A notable omission from the Guidelines is a discussion of what problems they are meant to address. In particular, it is important that they discuss questions such as the following: what is the impact of the present situation regarding the interplay between Article 3 and Chapter V? To what extent, and in what situations, can the rules of Article 3 and of Chapter V overlap? Does a duplication of protections create specific problems, or is it desirable to have multiple protections for international data processing? It is important that these points be discussed, in order to provide context for the positions taken in the Guidelines.

The following are some comments on particular issues raised in the Guidelines.

Specific Comments

Definition of international data transfer

The Guidelines define an international data transfer (p. 4) as involving 1) a controller or processor subject to the GDPR for the given processing, 2) disclosure of the data or making them available by this party to another controller or processor, and 3) a data importer located in a third country or an importer that is an international organisation.

Footnote 7 of the Guidelines suggest that this definition is based on the judgment of the CJEU in Case C-101/01 *Bodil Lindqvist* from 2003. However, the Court's holding in *Lindqvist* was limited to determining that the upload of data to a web site stored with a hosting provider established in the EU did not constitute an international data transfer under the former Directive 95/46 (see para. 71 of the judgment). Moreover, that case was decided before the Charter of Fundamental Rights was raised to the status of primary law in 2009 under Article 6(1) TEU. Since then the CJEU has relied on the Charter to emphasize the need for a high standard of protection for international data transfers in the context of international agreements of the EU (*Opinion 1/15*, paras. 119-231), Commission adequacy decisions (Case C-362/14 *Schrems*, paras. 38-40), and the EU standard contractual clauses (Case C-311/18 *Schrems*, para. 99).

In light of these judgments, any definition of international data transfers must be based on the necessity of providing a high level of protection, not on a single judgment decided many years ago under a different legal framework and different circumstances. The EDPB should explain how its definition fits with these recent judgments of the CJEU and the emphasis they put on ensuring a high level of protection under the Charter.

The consequences of the definition adopted in the Guidelines can be seen in Example 1 on pp. 5-6 of the Guidelines. In that example, the Singapore company created and controls the technical means (i.e., the company web site) by which Maria provides her data. The web site was set up so that the company can access the data of EU individuals in Singapore, and it is in control of the purpose and means of processing that cause them to be sent outside the EU. Moreover, as the Guidelines recognize (para. 10), there is nothing in the GDPR requiring that a data exporter be established in the EU for Chapter V to apply. This means that the company should be regarded as

a controller by providing the web site by means of which Maria's data are processed in Singapore. A dictionary definition of 'transfer' is 'to convey, carry, or send from one person or place to another', and it is clear that entering the data on the web site has resulted in them being sent from the EU to Singapore. Even if the company's ultimate processing of the data in Singapore is subject to the GDPR under Article 3(2), this would still seem not to cover the entering of data onto the web site by Maria, since it is stated in para. 12 that in such case 'there is no controller or processor sending or making the data available'. As discussed below, this will create a class of data processing for which there is no responsible data controller or processor.

In this regard, there seems to be a contradiction between paras. 10 and 12 of the Guidelines. In para. 10, it is said that a party subject to Article 3(2) 'will have to comply with Chapter V when transferring personal data to a third country', while in para. 12 it is stated that when data are disclosed directly by the data subject 'there is no controller or processor making the data available'. However, if a party is subject to the GDPR (including Chapter V) under Article 3(2), then why can this party not be considered a data exporter when it provides technical means (such as a web site) that cause the data of an EU individual to be made available to it in a third country?

While in such a situation some of the data transfer mechanisms contained in Chapter V will be unavailable (e.g., an individual like Maria could not sign up to BCRs), others could be used, such as if the company were to join an approved code of conduct or certification mechanism under Article 46(2)(e-f). Article 40(3) and Article 42(2) GDPR allow controllers and processors not subject to the GDPR to adhere to approved codes of conduct and certification mechanisms respectively, and it would seem strange if non-EU controllers and processors were not able to join codes of conduct and certification schemes set up under Article 46 to provide protection for data transfers.

Thus, a better response in Example 1 would be to say that Chapter V applies to the transfer to Singapore of Maria's data on the web form. While some data transfer mechanisms under Chapter V could not apply in this case (for example, BCRs and the standard contractual clauses (SCCs) are not suitable for use by individuals), others could be used (such as if she gives her valid consent to the transfer under Article 49(1)(a), or if codes of conduct or certification mechanisms are used under Article 46(2)). This would provide an incentive for non-EU companies to adopt such codes or set up such certification mechanisms, which could be designed in consultation with the EDPB.

Creating gaps in protection

The CJEU requires a high level of protection when EU personal data are processed or transferred abroad, as follows from its judgments mentioned above. Removing the protections of Chapter V from data that are transferred directly from individuals in the EU would create gaps in protection in several ways.

First of all, under the EDPB's definition of international data transfers there will be no data controller or data processor that is accountable in cases when a data subject sends her personal data to a non-EU controller or processor. The CJEU has held that

'the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data' (Case C-362/14 *Schrems*, para. 45), but under the EDPB's definition, the entry by individuals of their personal data onto Internet sites would fall into a legal 'no man's land' without any data controller or processor that can be held responsible. For example, information about the risks of transfers or the safeguards used must be provided under Articles 13(1)(f), 14(1)(f), 15(2), and Article 49(1)(a) GDPR when a data transfer occurs, but if the provision by an individual of her own data to a web site is deemed not to be a data transfer, then there will be no party to provide such information. An important term like 'data transfer' cannot be defined so restrictively as to result in data processing falling outside the protection of the GDPR.

Second, data transfer rules under Chapter V contain mechanisms that help compensate for the difficulty of enforcing obligations under EU law against parties in third countries. For example, in issuing an adequacy decision the Commission must ensure that data protection in the third country provides for 'effective and enforceable data subject rights and effective administrative and judicial redress' (Article 45(2)(a)) and that there is an independent supervisory authority with 'adequate enforcement powers' (Article 45(2)(b)); the SCCs contain clauses giving data subjects extra redress mechanisms against data importers;[2] and BCRs must contain various mechanisms to ensure effective enforcement, such as acceptance by the EU controller or processor of liability for breaches by non-EU members of the corporate group (Article 47(2)(f)) and the use of audit and verification procedures (Article 47(2)(j)). Many protections that apply under data transfer rules can also be enforced against the data exporter in the EU.[3] By contrast, when the GDPR applies to data processing in a third country it does so regardless of the level of protection or the possibility of enforcement. Thus, relying solely on the territorial application of the GDPR under Article 3(2) to protect data sent to third countries will remove many enforcement options.

The Guidelines attempt to address this enforcement deficit by suggesting that new SCCs be developed 'in cases where the importer is subject to the GDPR for the given processing in accordance with Article 3(2)' (p. 9). However, this does not seem to make sense, since in such cases 'there is no controller or processor sending or making the data available' (see p. 5) and thus no party capable of signing the SCCs as data exporter. It may be that here the EDPB is proposing a new set of SCCs to cover data transfers from non-EU parties subject to the GDPR that receive EU data and then transfer them on to third parties, but the language used is confusing. The Guidelines could also propose the development of codes of conduct and certification mechanisms with enhanced enforcement mechanisms to be adopted by non-EU parties that initiate data transfers from the EU.

Third, finding that data transfer rules do not apply to interactions between data subjects and non-EU parties would contradict the intent of the GDPR to discourage online monitoring of EU individuals (see Recital 24). Some companies may want to avoid signing SCCs or entering into other data transfer mechanisms and prefer having

---

[2] Annex to the Commission Implementing Decision on standard contractual clauses, Clauses 10-11.

[3] Ibid., Clause 2.

the GDPR apply to them under Article 3(2), since they know that the chances of enforcement outside the EU are higher under Chapter V than under Article 3. This would prove counterproductive by creating incentives for online monitoring.

Fourth, relying solely on territorial scope rules for protection creates practical problems that can impact the level of protection. Non-EU parties to data transfers may be able to manipulate the determination of whether or not they are subject to the GDPR to their advantage. For instance, parties in third countries that want to receive data from the EU could claim that they do not need to implement data transfer mechanisms since they are subject to the GDPR directly. This would put EU data exporters in the position of having to undertake an independent legal analysis of whether the GDPR applies to data processing by the importer, which would be practically infeasible and could subject them to unforeseeable liability risks.

Addressing the interplay of Article 3 and Chapter V in a future revision of the GDPR

Ideally the GDPR's rules on territorial scope and international data transfers should be combined in a single provision dealing with protection against external threats to EU data (some suggestions along these lines are contained in my Research Paper mentioned above). The interplay of Article 3 and Chapter V presents complex legal issues that arise from the failure to address this issue in the text of the GDPR, and cannot be completely resolved in EDPB guidelines. It is thus essential that in the Guidelines the EDPB call for this issue to be addressed in a future revision of the GDPR. In para. 23 the Guidelines already mention some of the issues that should be dealt with in a revision, such as avoiding duplication of provisions resulting from the application of Article 3 and Chapter V; addressing protections that are missing through the application of Article 3 alone; and ensuring that the sole application of Article 3 does not result in a gap in enforcement as compared to Chapter V.

Need for transparency and further discussion

It is important that the EDPB consider the issues concerning the interplay between Article 3 and Chapter V in a transparent fashion, and that in doing so it take account of expert opinion. It is commendable that the EDPB is holding a public consultation on the Guidelines, but there needs to be greater transparency surrounding its discussions on the topic.

Finally, the issues presented involve complex considerations of EU law, fundamental rights law, and international law, and the EDPB's work would benefit from obtaining expert input in a more focused way. The EDPB seems regularly to conduct discussions with large companies and holds 'FabLabs' with them to discuss its work; could it not also hold a FabLab for academics and other stakeholders (such as NGOs) to discuss the issues pertaining to the interplay of Article 3 and Chapter V?