

Comments by the Centre for Information Policy Leadership to the European Data Protection Board’s Draft Guidelines 05/2021 on the Interplay between Article 3 and Chapter V GDPR

On November 18, 2021, the European Data Protection Board (EDPB) issued its Draft 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 (Draft Guidelines). The EDPB invited public comments on this document and the Centre for Information Policy Leadership (CIPL)¹ appreciates the opportunity to submit the comments below as input for the final Guidelines.

CIPL welcomes the publication of the Draft Guidelines. As we previously underlined in our comments to the EDPB Guidelines 3/2018,² clarifying the interplay between territorial scope and Chapter V will be instrumental to the successful identification of the relevant tools and measures to adopt in the context of international transfers of personal data.

In our view, it is equally imperative that such clarifications are both legally robust and are also capable of practical implementation by businesses of all types and sizes. The objectives of protection of personal data can only be as successful as organizations’ ability to operationalize compliance: having organizations implement and accumulate different layers of compliance obligations with increasing complexity may ultimately run counter to practical compliance and accountability. In other words, stretching the criteria which trigger the application of the GDPR too far, or accumulating additional layers of complexity, will mean running the risk of facilitating a “paper based” or “blind blanket adoption” of SCCs for mere formal compliance purposes, neutralizing every effort of actual protection of personal data in international transfers.

CIPL also welcomes the inclusion of many specific examples that follow up and elaborate on the ones already used in Guidelines 3/2018³. As we did in that earlier submission, we re-propose an updated chart of different possible scenarios to summarize the GDPR’s territorial scope at a glance. This should assist organizations, in particular, SMEs and other stakeholders such as DPAs to quickly assess whether and to what extent organizations are subject to the GDPR and transfer requirements (See chart in Annex 1). CIPL recommends including this chart in the Final Guidelines.

¹ CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL’s mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL’s work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL’s website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

² [CIPL Comments on the EPDB’s Territorial Scope Guidelines](#) January 18, 2019. In this answer, CIPL comments will also reflect and follow up observations we already published and submitted, in particular CIPL White Paper—[A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision](#), September 24, 2020; [CIPL Comments on the EDPB’s Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#), December 21, 2020.

³ EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3).

COMMENTS

In our earlier comments to the EDPB Guidelines 3/2018,⁴ we made a number of recommendations, which included recommendations to (1) explain the relationship between Article 3 and Chapter 5 of the GDPR and (2) clarify that Chapter V of the GDPR does not apply to organizations subject to the GDPR under Article 3(2). In response to the Draft Guidelines, we have the following further comments on these two recommendations, and other comments.

Initially, as a general comment, we believe that the presented definition of transfer in the Draft Guidelines does not reflect the spirit and ambitions of the GDPR.⁵ As a consequence of this interpretation, organizations will be required to accumulate and implement yet another layer of compliance obligations. If an organization is acting within the scope of Article 3(2), it is already required to put in place all the measures and safeguards of the GDPR; hence there is no added value for data subjects or organizations in requiring organizations to additionally comply with the obligations of Chapter V.⁶

We are pleased to see that the EDPB Guidelines 5/2021 address the issue of the relationship between Article 3 and Chapter V of the GDPR. However, we would like to point out the need for further clarification on a number of issues. Specifically:

Example 1: Controller in a third country collects data directly from a data subject in the EU:

- We welcome confirmation that where data are disclosed on the own initiative of a data subject, that this does not constitute a transfer that needs to be “legitimized” under Chapter V.
- Our understanding of the part of the example where it states: “*the Singaporean company will need to check whether its processing operations are subject to the GDPR pursuant to Article 3(2).*” is that it is intended to clarify that the recipient in the example is not targeting or monitoring the data subject, which would otherwise result in GDPR applying to the recipient.
- We encourage EDPB to provide additional clarity on how the transfer guidance would apply to multiparty/simultaneous scenarios, such as consolidated data for regulatory or risk reporting or data ecosystems like Gaia-X, where data may be hosted and accessed frequently by multiple parties, sometimes downloaded or copied or just viewed in the case of a data resource such as an HR or CRM database.

⁴ [CIPL Comments on the EPDB’s Territorial Scope Guidelines](#) January 18, 2019.

⁵ 2019 CIPL Comments “Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3).”

⁶ Id.

Examples 5 and 6:

Example 5 provides a helpful clarification in the example of an employee taking a laptop outside of the EU and accessing personal data, which would not be regarded as a transfer under Chapter V. Following the same logic, in Example 6, it would be helpful to reflect the legal reality of branches forming part of the same legal person as the head office, and the practical reality of daily data flows within and among branches and parent companies.

- More specifically, if an EU entity has a branch office in a third country, it is difficult to see how SCCs could be concluded with a branch that does not have a separate legal personality.
- Paragraphs 17 and 24 specify that, although a certain data flow may not qualify as a “transfer” to a third country, this processing can still be associated with risks. The controller being accountable for its processing activities (including Articles 24, 32, 33, 35, and 48), may conclude that extensive security measures are needed, or even that it would not be lawful to conduct or proceed with the specific processing operation in a third country based on wider GDPR requirements, although there is no “transfer” situation.
 - Should the controller in this case perform a separate specific assessment (along the lines of a DPIA) of the risks in order to decide whether to proceed with the processing?
 - If so, could the EDPB clarify which conditions (including the existence of any appropriate supplementary measures) are required to further protect the personal data involved?
 - Would the assessment of the above-mentioned risks be included in controller’s endeavors to observe its accountability obligations under GDPR?
 - Additionally, this suggestion will introduce tremendous confusion to the challenging situations companies are already facing, particularly companies with less resources, and will undermine the validity and importance of the adequacy status of the 15 third countries currently being relied upon for a vast number of these “non-transfers.” For example, based on this suggestion in the draft guidance, all Canadian, Japanese or Swiss controllers who have been “transferring” EU data to themselves, would be left in doubt as to whether they could continue to rely on the adequacy status of their respective countries. To avoid this, we suggest either:
 - the deletion of the above-mentioned language in paragraph 17, or
 - alternatively, if the EDPB decides to maintain this language, it should be augmented with a clarification that the adequacy of a third country and safeguards similar as those enumerated in Article 46 of the GDPR will be a relevant factor, even if there is a no “transfer” situation.
 - The EDPB should also clarify that the risk-based approach and Articles 24 and 32 of the GDPR require technical and organizational measures, but not necessarily the Supplementary Measures outlined by the EDPB’s recommendations when applying Standard Contractual Clauses for an international data transfer.

Example 3: Processor in the EU sends data back to the original controller in a third country

This example generates a number of complexities and concerns:

“XYZ Inc., a controller without an EU establishment, sends personal data of its employees/customers, all of them non-EU residents, to the processor ABC Ltd. for processing in the EU, on behalf of XYZ. ABC re-transmits the data to XYZ. The processing performed by ABC, the processor, is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since ABC is established in the EU. Since XYZ is a controller in a third country, the disclosure of data from ABC to XYZ is regarded as a transfer of personal data and therefore Chapter V applies.”

- The residency of the data subjects is irrelevant for the application of the GDPR. For clarity, the first sentence in the above paragraph should read *“XYZ Inc., a controller established outside the EU, whose processing of personal data of its employees/customers is not subject to the GDPR, sends that personal data to the processor ABC Ltd.”*
- It is clear that *“The processing performed by ABC, the processor, is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since ABC is established in the EU.”* But the following sentence *“Since XYZ is a controller in a third country, the disclosure of data from ABC to XYZ is regarded as a transfer of personal data and therefore Chapter V applies”* creates some concerns:
 - Firstly, *semantically* a “disclosure of data” implies that the recipient of the disclosed data does not or did not already have that data. In this example, ABC merely *“re-transmits the data to XYZ” – processors merely return the data to the controller or provides the data outcomes of a data processing operation back to the controller.*
 - Secondly, the application of Chapter V to the re-transmission of data from ABC to XYZ imposes significant additional burdens on EU processors processing non-EU data. XYZ processing operations are not subject to the GDPR. XYZ does not expect the scrutiny and additional safeguards of Chapter V to apply to a mere re-transmission of its own data. Data subjects whose data is controlled by XYZ expect that their personal data will be processed in accordance with the laws applicable to XYZ in their jurisdiction. Finally, the additional burdens imposed by applying Chapter V requirements would significantly undermine the competitiveness of EU based service providers processing non-EU personal data on behalf and on instructions of foreign controllers. They will be required to implement data protection standards that are not known to or even expected by the data subjects in the first place, nor would they be expected by the controller. Indirectly, this may create reticence for foreign controllers to engage EU based processors for fear of additional administrative burdens, controls and processes that would apply to their originally outsourced data.

- Section 3 “*Consequences*” notes that if there is a transfer to a third country⁷, the controller or processor needs to comply with the conditions of Chapter V and frame the transfer by using the instruments aimed at protecting personal data after they have been transferred⁸ - namely those foreseen in Articles 45, 46 and 49⁹. However, paragraph 23¹⁰ specifies that “*for a transfer of personal data to a controller in a third country less protection/safeguards are needed if such controller is already subject to the GDPR for the given processing. Therefore, when developing relevant transfer tools (which currently are only available in theory) i.e. standard contractual clauses or ad hoc contractual clauses, the Article 3(2) situation should be taken into account in order not to duplicate the GDPR obligations but rather to address the elements and principles that are “missing” and, thus, needed to fill the gaps [...]*”. In fact, the European Commission has confirmed that, after the draft guidelines are adopted, it intends to develop a specific set of SCCs regarding transfers to importers subject to Article 3(2) GDPR¹¹.
 - Could the EDPB further elaborate on what entities should do in case of transfers of personal data to a controller that is already subject to the GDPR for the given processing while this new specific set of SCCs is being developed? This would build legal certainty for organizations ahead of the publication by the European Commission of the new ad hoc SCCs.
 - Could the EDPB also provide specific examples of how *Article 3(2) situation should be taken into account in order not to duplicate the GDPR obligations*?
 - Could the EDPB also clarify the (although theoretical) interplay between the current SCCs and the specific set of SCCs? In particular: the implementation of specific SCCs shouldn't be required if the existing SCCs are already in place.

⁷ EDPB Draft 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 paragraph 19

⁸ Id. Paragraph 20

⁹ Id. Paragraphs 21 and 22: the existence of an adequate level of protection in the third country, or appropriate safeguards as Standard Contractual Clauses (SCCs): Binding Corporate Rules (BCRs); Codes of conduct; Certification mechanisms; Ad hoc contractual clauses or derogations for specific situations

¹⁰ Id.

¹¹ EDPB 54th Plenary meeting Minutes, 14 September 2021 point 2.1

RECOMMENDATIONS

As we previously noted, the objectives of protection of personal data can only be as successful as organizations' ability to operationalize compliance in a responsible and accountable manner. Having organizations implement and accumulate multiple and different layers of compliance obligations with increasing complexity may ultimately create hurdles to effective compliance and accountability. Importantly, it would divert much needed privacy and legal resources within organizations from other, and arguably more impactful, compliance and accountability activities, such as compliance with transparency, data protection principles, conducting risk assessments and DPIA, ensuring privacy by design of services and products. In this regard, we would like to submit the following further recommendations.

The EDPB should consider:

- A. Allowing organizations to make the most of the Chapter V toolbox—i.e., consider outcome- based contractual measures and ad hoc clauses and other measures, such as certification schemes and codes of conduct, leaving it to the parties to work out and agree on the appropriate contractual structure and procedural formalities, subject to an overriding obligation that the measures must be legally binding on the parties involved and give appropriate third-party rights.
- B. Allowing organizations to implement and reflect their own risk-based organizational accountability frameworks and to align (1) with the CJEU's mandate to look at the full context of a transfer and (2) with the GDPR's requirement to consider the risks of varying likelihood and severity to the rights and freedoms of individuals. The risk assessments require a holistic approach, whereby no criterion by itself may be decisive for the outcome of the analysis. They should be based on empirical evidence, including previous history of government access requests and other criteria. Considering this kind of empirical evidence would be an objective standard.
- C. Take into account the supplementary measures adopted by organizations to mitigate risks in data transfers. These supplementary measures are a combination of legal, organizational and technical measures. Consistent with the risk-based approach and Articles 24 and 32 of the GDPR, these measures are calibrated on a case-by-case basis to the severity and likelihood of risk of harm to individuals. The mitigating impact of each of these measures may differ depending on the risk being addressed. Therefore, not all of these measures should be required or considered appropriate in every instance and for all organizations. Several of these measures have already been or are being implemented by organizations as part of their accountability measures under the GDPR. As stated above, the EDPB should also clarify that the risk-based approach and Articles 24 and 32 of the GDPR require technical and organizational measures, but not necessarily the Supplementary Measures outlined by the EDPB's recommendations when applying Standard Contractual Clauses for an international data transfer.
- D. Recognize that there are situations where organizations can rely on Article 49 GDPR derogations, as they have been rightfully provided and enabled in the GDPR as legitimate derogations from a rule.

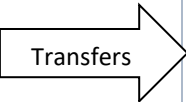
CONCLUSION

CIPL is grateful for the opportunity to provide comments on key interpretation questions of the territorial scope of the GDPR under Article 3. We look forward to providing further input as the Guidelines are finalized.

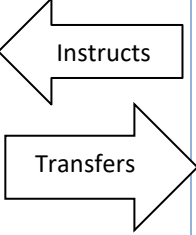
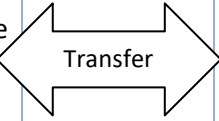
If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, or Camilla Ravazzolo cravazzolo@HuntonAK.com

ANNEX 1

Guidelines 3/2018 on Territorial Scope	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
	<p style="text-align: center;">Criteria to qualify as transfer:</p> <ol style="list-style-type: none"> 1) Controller or Processor subject to the GDPR for the given processing. 2) “Exporter” discloses personal data, subject to this processing, available to “Importer” 3) The importer is in a third country irrespective of whether or not is subject to the GDPR ex Article 3 or 3(2)

	EU	EU BORDER	THIRD COUNTRY	
CASE A	Data subject		Controller	<p>✘ Does not qualify as transfer ex Chapter V</p> <p>? GDPR application to be checked against processing operations</p>
CASE 1	<p>Controller Instructs Processor</p> <p>✓ GDPR applies to the controller ex Art. 3(1)</p>			

CASE 2 +	<p>Controller</p> <p>✓ GDPR applies to the controller ex Art. 3(1)</p>	<p>Instructs</p> <p>Transfers</p>	<p>Processor</p> <p>Processor is bound by Art. 28 GDPR</p>	<p>✓ Qualifies as Transfer ex Chapter V</p>
CASE 3 +	<p>Processor</p> <p>✓ GDPR applies to the processor ex Art. 3(1)</p>	<p>Instructs</p> <p>Transfers back</p>	<p>Controller</p> <p>Controller not otherwise subject to Art. 3(2) GDPR</p> <p>✗ GDPR does not apply</p>	<p>✓ Qualifies as Transfer ex Chapter V</p> <p>Exporter (P) discloses personal data to the importer (C) in a third country</p>
CASE B	<p>Processor</p> <p>✓ GDPR applies to the processor ex Art. 3(1)</p>	<p>Transfers</p>	<p>SUB - Processor</p>	<p>✓ Qualifies as Transfer ex Chapter V</p> <p>Exporter (P) discloses personal data to the importer (S-P) in a third country</p>
CASE C	<p>Controller</p> <p>✓ GDPR applies to the controller ex Art. 3(1)</p>		<p>Employee accesses databases</p>	<p>✗ Does not qualify as transfer ex Chapter V</p> <p>Employee is <i>integral part</i> of Controller</p>
CASE C +	<p>Controller (branch)</p> <p>✓ GDPR applies to the controller ex Art. 3(1)</p>	<p>Transfers</p>	<p>Processor (parent company)</p>	<p>✓ Qualifies as Transfer ex Chapter V</p> <p>For the specific processing activities subsidiary and parent company are defined as C and P. In this framework (C) discloses personal data to the importer (P) in a third country.</p>

Guidelines 3/2018			Guidelines 05/2021	
	EU	EU BORDER	THIRD COUNTRY	
CASE 4 +	Processor ✓ GDPR applies to the processor <i>ex Art. 3(1)</i>		Controller offering goods/services or monitoring subjects in the Union ✓ GDPR applies to the controller <i>ex Art. 3(2)</i>	✓ Qualifies as Transfer <i>ex Chapter V</i>
CASE D	Controller ✓ GDPR applies to the controller <i>ex Art. 3(1)</i>		Controller ✓ GDPR applies to the controller <i>ex Art. 3(2)</i>	✓ Qualifies as Transfer <i>ex Chapter V</i>
CASE 5			Controller Processor ✓ GDPR applies to the controller <i>ex Art. 3(2)</i>	Transfer <i>ex Chapter V</i>