To whom it may concern,

The Data Protection Office of the International Committee of the Red Cross (ICRC) welcomes the opportunity to provide input and feedback with reference to the 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*.
The ICRC Data Protection Office is the entity that is responsible, and entrusted with the necessary authority, for independently supervising the application of the ICRC Rules on Personal Data Protection at the ICRC, ensuring their consistent application across all ICRC activities.

We are particularly grateful for the opportunity to bring to your attention our observations, aimed at ensuring that the specific status of international organisations (IOs) is adequately reflected, in order to avoid potential misunderstandings in the interpretation of these Guidelines, and of the GDPR overall. Specifically, we are concerned that the current formulation of the Guidelines might generate some confusion over the position of IOs vis-à-vis the EU data protection framework and its applicability.

It is worth recalling that the EU Commission has clarified, when discussing the application of the GDPR in respect of cooperation with international organisations, that "The GDPR does not apply to international organisations (IOs), even when located in the EU, because of their specific Privileges and Immunities.".[1] This position is reiterated by the European Data Protection Board in their Guidelines 3/2018 *on the territorial scope of the GDPR (Article 3)*, where it is emphasised that "the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic missions and consular posts, as well as international organisations.".[2] The rationale behind the regulation of data transfers to third countries or to IOs through the additional protections required by the provisions of Chapter V GDPR is therefore a protective one (as emphasised by Recital 101 of the GDPR): it aims to ensure that the level of protection guaranteed to personal data by the GDPR is not undermined once these data are transferred to International Organizations or third countries, i.e. jurisdictions where the GDPR cannot be enforced.

In this respect, the GDPR equates, throughout its text and in particular in Chapter V, IOs to third countries, essentially treating IOs in the same way as sovereign third States for the purposes of data transfer mechanisms. In so far as IOs are concerned, indeed, once a transfer to an IO is undertaken, the personal data in question would come within the scope of the IO's applicable privileges and immunities (including inviolability of the IO's property, assets and archives, immunity from jurisdiction, and immunity from any other form of interference, whether by executive, administrative, judicial or legislative action),[3] effectively putting in place a procedural "barrier" from the enforcement of the

[1] Summary Record of 15th meeting of the Asylum, Migration and Integration and Internal Security Funds Committee of 5 February 2019, p.7, available at https://ec.europa.eu/transparency/comitology-register/screen/documents/061562/1/consult?lang=en.
[2] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), p. 23, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.
[3] Comments of the United Nations Secretariat on behalf of the United Nations System Organizations on the "Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies" adopted by the European Data Protection Board on 18 January 2020, of 14 May 2020, pp. 14-15, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf.

GDPR (or any other domestic data protection legislation). From this perspective, IOs would essentially be acting as their own "jurisdiction", and the only data protection framework applicable (and enforceable) to them would be their own rules and regulations, and not the laws of the State(s) where they operate or are located.

The purpose, and object, of Art 3(2) GDPR is very different, as it mentions neither IOs, nor third countries. Instead, it addresses "controllers or processors not established in the Union, where the processing activities are related to: (a) the offering of goods and services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union". This does create possible overlaps and questions as to the interpretation of the GDPR for cases in which an entity that is not established in the EU is required to apply the GDPR by virtue of Art 3(2), and also needs to receive data. In particular, it may legitimately be asked whether in such cases, Chapter V applies for transfers to such entities, despite them already being required to apply the GDPR by virtue of 3(2).
This potential doubt is however not applicable to "Third countries or IOs", which, as mentioned above, abide by their own regulatory frameworks exclusively: the protections of Article V will therefore remain relevant and necessary in cases of transfers to them, following the logic of Recital 101 GDPR.

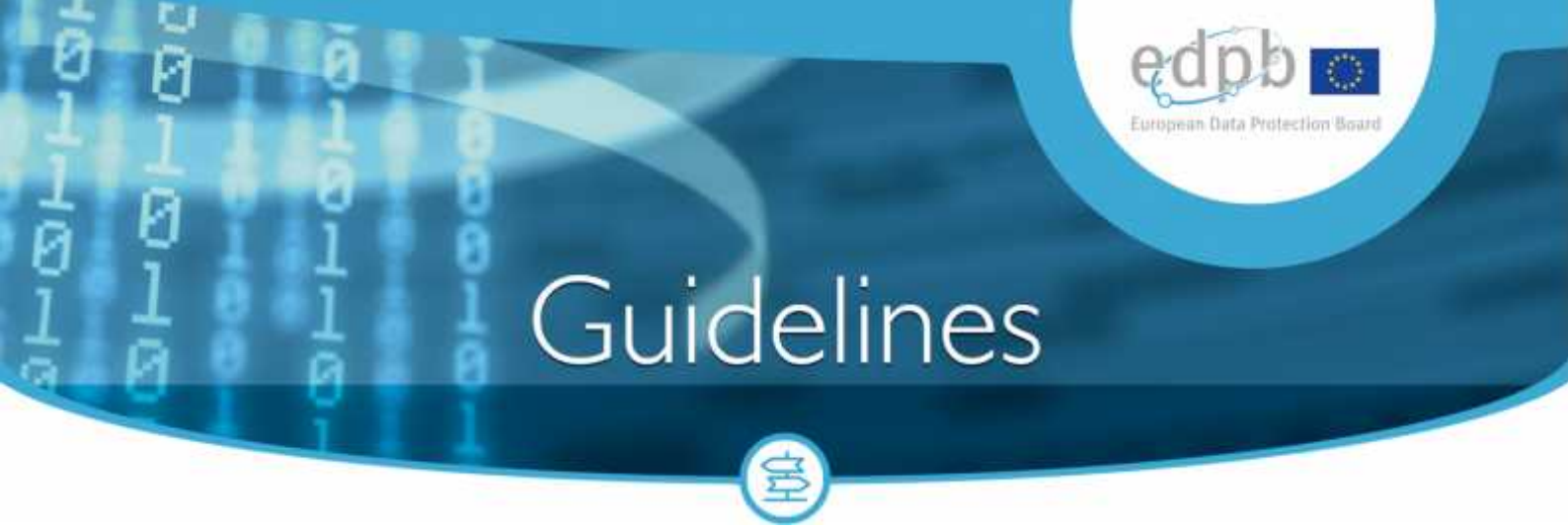
The current formulation of Guidelines 5/2020, however, seems to conflate IOs with "controllers or processors not established in the Union", as referred to in Art 3 GDPR, rather than with "third countries", in line with Chapter V GDPR (see, for instance, section 2.3 of the Draft Guidelines).
This apparent assimilation to a private/commercial entity established outside of the Union seems to imply that an IO may be compelled to apply the GDPR, much like any private entity established in a third country, by virtue of the application of article 3 GDPR. Such application would however be incompatible with applicable privileges and immunities enjoyed by IOs, and seems to contradict both the EU Commission's position and the EDPB Guidelines 3/2018, referenced above.
As a consequence, such a formulation is arguably inconsistent with the logic of treating IOs in a way that is comparable to third countries, which underpins Chapter V and the GDPR more widely. We are therefore concerned that it may lead to overall confusion over the status of IOs and their relationship to the GDPR (discussions that IOs anyway still encounter frequently when dealing with private/commercial entities who are not used to negotiating contracts with IOs).

We have therefore suggested some reformulations throughout the Draft Guidelines to provide further clarity and avoid misunderstandings, and we hope that you may find it useful for the finalisation of the document.

We remain available in case of any further doubt or unclarity, and we look forward to continuing to work together.

Best regards,

ICRC Data Protection Office



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

Adopted on 18 November 2021

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter the "GDPR" or "Regulation"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

1 INTRODUCTION

1. According to Article 44of the GDPR,[2] the conditions laid down in its Chapter V shall apply to any "transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation".[3] The overarching purpose of Chapter V is to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data are transferred "to third countries or to international organisations".[4]

2. The provisions of Chapter V aim at ensuring the continued protection of personal data after they have been transferred to a third country or to an international organisation. When personal data is processed on EU territory it is protected not only by the rules in the GDPR but also by other rules, both on EU and Member State level, that must be in line with the GDPR (including possible derogations therein) and ultimately with the EU Charter on fundamental rights and freedoms. When personal data is transferred and made accessible to entities outside the EU territory, the overarching legal framework provided within the Union no longer applies.

3. Therefore, it must be ensured that the transferred personal data is protected in other ways, such as by being transferred in the context of an adequacy decision from the European Commission or by provision of appropriate safeguards in accordance with Chapter V of the GDPR. When relying on one of the transfer tools listed in Article 46 GDPR, it must be assessed whether supplementary measures need to be implemented in order to bring the level of protection of the transferred data up to the EU

[1] References to "EU" and "Member States" made throughout this document should be understood as references to "EEA" and "EEA Member States" respectively.
[2] "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation."
[3] "International organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
[4] Besides Recital 101, this is particularly emphasized by Article 44, sentence 2 which reads: "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

standard of essential equivalence.[5] This applies also in situations where the processing falls under Article 3(2) of the GDPR, in order to avoid that the protection provided by the GDPR is undermined by other legislation that the importer falls under. This may for example be the case where the third country has rules on government access to personal data that go beyond what is necessary and proportionate in a democratic society (to safeguard one of the important objectives as also recognised in Union or Member States' law, such as those listed in Article 23(1) GDPR). The provisions in Chapter V are there to compensate for this risk and to complement the territorial scope of the GDPR as defined by Article 3 when personal data is transferred to countries outside the EU.

4. The following sections aim at clarifying this interplay between Article 3 and the provisions of the GDPR on international transfers in Chapter V in order to assist controllers and processors in the EU in identifying whether a processing constitutes a transfer to a third country or to an international organisation and, as a result, whether they have to comply with the provisions of Chapter V of the GDPR.

5. It is however important to keep in mind that although a certain data flow may not constitute a transfer under Chapter V, such processing can still be associated with risks for which safeguards must be envisaged. Regardless of whether the processing takes place in the EU or not, controllers and processors always have to comply with all relevant provisions of the GDPR, such as the Article 32 obligation to implement technical and organizational measures taking into account, *inter alia*, the risks with respect to the processing.

2 CRITERIA TO QUALIFY A PROCESSING AS A TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANISATION

6. Since the GDPR does not provide for a legal definition of the notion "transfer of personal data to a third country or to an international organisation",[6] it is essential to clarify this notion.

7. The EDPB has identified[7] the three following cumulative criteria that qualify a processing as a transfer:

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

    2) This 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").

    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.

[5] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
[6] Article 44, sentence 1.
[7] Having regard to relevant findings in the CJEU Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596.

8. It is useful to recall here that pursuant to Article 3, the application of the GDPR must always be assessed in relation to a certain processing rather than with regard to a specific entity (e.g. a company).[8]

2.1 A controller or a processor is subject to the GDPR for the given processing

9. The first criterion requires that the processing at stake meets the requirements of Article 3 GDPR, i.e. that a controller or processor is subject to the GDPR for the given processing. This has been further elaborated on in the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

10. It is worth underlining that controllers and processors, which are not established in the EU, may be subject to the GDPR pursuant to Article 3(2) for a given processing and, thus, will have to comply with Chapter V when transferring personal data to a third country or to an international organisation.

2.2 This 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")

11. The second criterion requires that there is a controller or processor disclosing by transmission or otherwise making data available to another controller or processor. These concepts have been further elaborated on in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. It should, *inter alia*, be kept in mind that the concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law. A case-by-case analysis of the processing at stake and the roles of the actors involved is necessary.[9]

12. This second criterion cannot be considered as fulfilled where the data are disclosed directly and on his/her own initiative by the data subject[10] to the recipient. In such case, there is no controller or processor sending or making the data available ("exporter").[11]

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

Maria, living in Italy, inserts her personal data by filling a form on an online clothing website in order to complete her order and receive the dress she bought online at her residence in Rome. The online clothing website is operated by a company established in Singapore with no presence in the EU. In this case, the data subject (Maria) passes her personal data to the Singaporean company, but this does not constitute a transfer of personal data since the data are not passed by an exporter (controller or processor), since they are passed directly and on her own initiative by the data subject herself. Thus,

[8] See Sections 1–3 of the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).
[9] See page 9 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[10] The data subject cannot be considered a controller or processor. This follows from Article 4(10) GDPR which differentiates between controller/processor and data subject. Hence, a data subject disclosing his/her own personal data cannot be considered an "exporter". This is without prejudice to the fact that a natural person/an individual can be a controller/processor in accordance with Article 4(7) and 4(8) GDPR (e.g. as a self-employed person). However, this does not limit the protection that natural persons acting as a controller/processor enjoy where their own personal data are concerned.
[11] In addition, it is important to recall that where the processing of personal data is carried out "by a natural person in the course of a purely personal or household activity", such processing will, in accordance with Article 2(2)(c), fall outside the material scope of the GDPR.

Chapter V does not apply to this case. Nevertheless, the Singaporean company will need to check whether its processing operations are subject to the GDPR pursuant to Article 3(2).[12]

Example 2: Controller in the EU sends data to a processor in a third country

Company X established in Austria, acting as controller, provides personal data of its employees or customers to a company Z established in Chile, which processes these data as processor on behalf of X. In this case, data are provided from a controller which, as regards the processing in question, is subject to the GDPR, to a processor in a third country. Hence, the provision of data will be considered as a transfer of personal data to a third country and therefore Chapter V of the GDPR applies.

13. It is also important to note that Article 44 of the GDPR clearly envisages that a transfer may not only be carried out by a controller but also by a processor. Therefore, there may be a transfer situation where a processor sends data to another processor or even to a controller as instructed by its controller.

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

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.

Example 4: Processor in the EU sends data to a sub-processor in a third country

Company A established in Germany, acting as controller, has engaged B, a French company, as a processor on its behalf. B wishes to further delegate a part of the processing activities that it is carrying out on behalf of A to sub-processor C, a company established in India, and hence to send the data for this purpose to C. The processing performed by both A and its processor B is carried out in the context of their establishments in the EU and is therefore subject to the GDPR pursuant to its Article 3(1), while the processing by C is carried out in a third country. Hence, the passing of data from processor B to sub-processor C is a transfer to a third country, and Chapter V of the GDPR applies.

14. The second criterion implies that the concept of "transfer of personal data to a third country or to an international organisation" only applies to disclosures of personal data where two different (separate) parties (each of them a controller, joint controller or processor) are involved. In order to qualify as a transfer, there must be a controller or processor disclosing the data (the exporter) and a different controller or processor receiving or being given access to the data (the importer).

Example 5: Employee of a controller in the EU travels to a third country on a business trip

George, employee of A, a company based in Poland, travels to India for a meeting. During his stay in India, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This remote access of personal data from a third country, does not qualify as a

[12] In this regard, see Recital 23, which includes elements to be assessed when determining whether the targeting criterion in Article 3(2)(a) GDPR is met.

transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (company A). Therefore, the disclosure is carried out within the same controller (A). The processing, including the remote access and the processing activities carried out by George after the access, are performed by the Polish company, i.e. a controller established in the Union subject to Article 3(1) of the GDPR.

15. Hence, if the sender and the recipient are not different controllers/processors, the disclosure of personal data should not be regarded as a transfer under Chapter V of the GDPR – since data is processed within the same controller/processor. In this context, it should be kept in mind that controllers and processors are nevertheless obliged to implement technical and organisational measures, considering the risks with respect to their processing activities, in accordance with Article 32 of the GDPR.

16. It should also be recalled that entities which form part of the same corporate group may qualify as separate controllers or processors. Consequently, data disclosures between entities belonging to the same corporate group (intra-group data disclosures) may constitute transfers of personal data.

Example 6: A subsidiary (controller) in the EU shares data with its parent company (processor) in a third country

The Irish Company A, which is a subsidiary of the U.S. parent Company B, discloses personal data of its employees to Company B to be stored in a centralized HR database by the parent company in the U.S. In this case the Irish Company A processes (and discloses) the data in its capacity of employer and hence as a controller, while the parent company is a processor. Company A is subject to the GDPR pursuant to Article 3(1) for this processing and Company B is situated in a third country. The disclosure therefore qualifies as a transfer to a third country within the meaning of Chapter V of the GDPR.

17. Although a certain data flow may not qualify as a "transfer" to a third country in accordance with Chapter V of the GDPR, including example 5, such processing can still be associated with risks, for example due to conflicting national laws or government access in a third country as well as difficulties to enforce and obtain redress against entities outside the EU. The controller is accountable for its processing activities, regardless of where they take place, and must comply with the GDPR, including Article 24 ("Responsibility of the controller"), 32 ("Security of processing"), 33 ("Notification of a personal data breach"), 35 ("Data Protection Impact Assessment"), 48 ("Transfers or disclosures not authorised by Union law"), etc. Following from its obligation to implement technical and organisational measures taking into account, *inter alia*, the risks with respect to the processing under Article 32 of the GDPR, a controller may very well conclude that extensive security measures are needed – or even that it would not be lawful – to conduct or proceed with a specific processing operation in a third country although there is no "transfer" situation. For example, a controller may conclude that employees cannot bring their laptops, etc. to certain third countries.

2.3 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

18. The third criterion requires that the importer is geographically in a third country or is an international organisation, but regardless of whether the processing at hand falls under the scope of the GDPR.

Example 7: Processor in the EU sends data back to its controller in a third country

Company A, a controller without an EU establishment, offers goods and services to the EU market. The French company B, is processing personal data on behalf of company A. B re-transmits the data to A. The processing performed by the processor B is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since it takes place in the context of the activities of its establishment in the EU. The processing performed by A is also covered by the GDPR, since Article 3(2) applies to A. However, since A is in a third country, the disclosure of data from B to A is regarded as a transfer to a third country and therefore Chapter V applies.

3 CONSEQUENCES

19. If all of the criteria as identified by the EDPB are met, there is a "transfer to a third country or to an international organisation". Thus, a transfer implies that personal data are sent or made available by a controller or processor (exporter) which, regarding the given processing, is subject to the GDPR pursuant to Article 3, to a different controller or processor (importer) in a third country, regardless of whether or not this importer is subject to the GDPR in respect of the given processing.

20. As a consequence, the controller or processor in a "transfer" situation (according to the criteria described above) needs to comply with the conditions of Chapter V and frame the transfer by using the instruments which aim at protecting personal data after they have been transferred to a third country or an international organisation.

21. These instruments include the recognition of the existence of an adequate level of protection in the third country or international organisation to which the data is transferred (Article 45) or, in the absence of such adequate level of protection, the implementation by the exporter (controller or processor) of appropriate safeguards as provided for in Article 46.[13] According to Article 49, personal data can be transferred to a third country or an international organisation without the existence of an adequate level of protection or the implementation of appropriate safeguards only in specific situations and under certain conditions.

22. The main types of transfer tools listed in Article 46 are:

- Standard Contractual Clauses (SCCs).
- Binding Corporate Rules (BCRs).
- Codes of conduct.
- Certification mechanisms.
- Ad hoc contractual clauses.
- International agreements/Administrative arrangements.

23. The content of the safeguards needs to be customized depending on the situation. As an illustration, the guarantees to be provided for a transfer of personal data by a processor are not the same as the

[13] In this context, see also the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

ones to be provided for a transfer by a controller.[14] Similarly, 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 relating to conflicting national laws and government access in the third country as well as the difficulty to enforce and obtain redress against an entity outside the EU. To clarify, such tools should, for example, address the measures to be taken in case of conflict of laws between third country legislation and the GDPR and in the event of third country legally binding requests for disclosure of data. The EDPB encourages and stands ready to cooperate in the development of a transfer tool, such as a new set of standard contractual clauses, in cases where the importer is subject to the GDPR for the given processing in accordance with Article 3(2).

24. To summarize, if the criteria as identified by the EDPB are not met, there is no "transfer" and Chapter V of the GDPR does not apply. As already mentioned, a controller is nonetheless accountable for all processing that it controls, regardless of where it takes place, and data processing in third countries may involve risks which need to be identified and handled (mitigated or eliminated, depending on the circumstances) in order for such processing to be lawful under the GDPR.

25. It is worth underlining that controllers and processors whose processing is subject to the GDPR pursuant to Article 3 always have to comply with Chapter V of the GDPR when they disclose personal data to a controller or processor in a third country or to an international organisation. This also applies to disclosures of personal data carried out by controllers/processors which are not established in the EU but are subject to the GDPR pursuant to Article 3(2) to a controller or processor in the same or another third country.

[14] Cf. 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.