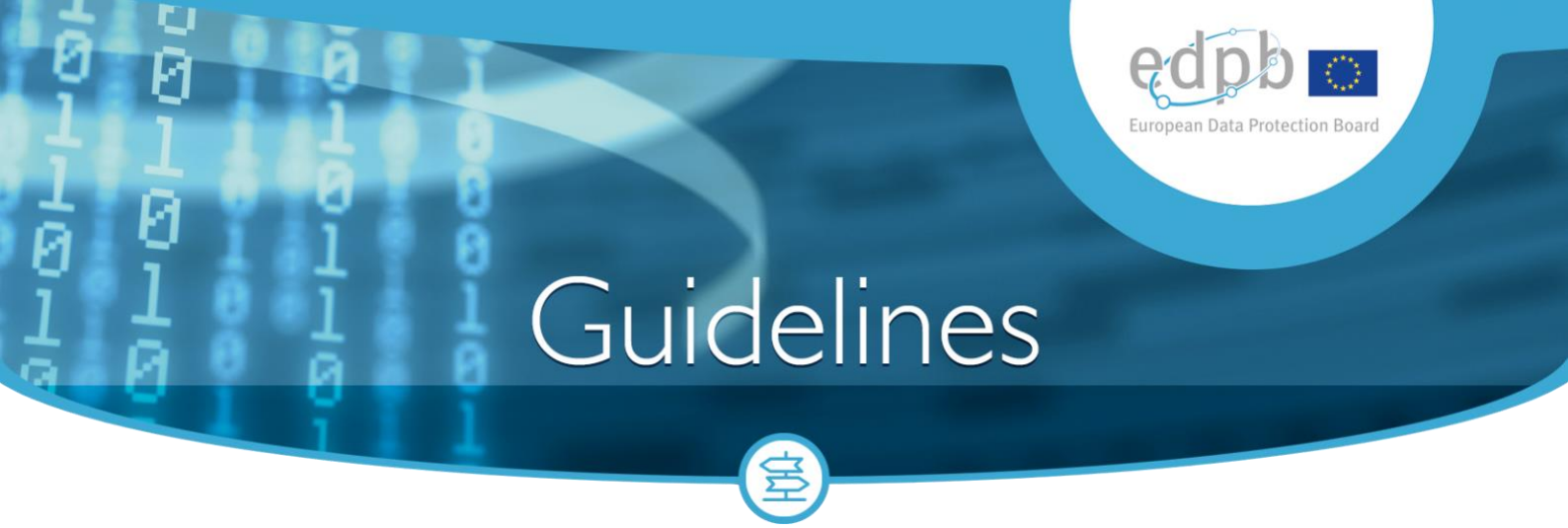


Guidelines 02/2024 on Article 48 GDPR

Adopted on 02 December 2024

EXECUTIVE SUMMARY

Article 48 GDPR provides that: "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter*".

The purpose of these guidelines is to clarify the rationale and objective of this article, including its interaction with the other provisions of Chapter V of the GDPR, and to provide practical recommendations for controllers and processors in the EU that may receive requests from third country authorities to disclose or transfer personal data.

The main objective of the provision is to clarify that judgments or decisions from third country authorities cannot automatically and directly be recognised or enforced in an EU Member State, thus underlining the legal sovereignty vis-a-vis third country law. As a general rule, recognition and enforceability of foreign judgements and decisions is ensured by applicable international agreements.

Regardless of whether an applicable international agreement exists, if a controller or processor in the EU receives and answers a request from a third country authority for personal data, such data flow is a transfer under the GDPR and must comply with Article 6 and the provisions of Chapter V.

An international agreement may provide for both a legal basis (under Article 6(1)(c) or 6(1)(e)) and a ground for transfer (under Article 46(2)(a)).

In the absence of an international agreement, or if the agreement does not provide for a legal basis under Article 6(1)(c) or 6(1)(e), other legal bases could be considered. Similarly, if there is no international agreement or the agreement does not provide for appropriate safeguards under Article 46(2)(a), other grounds for transfer could apply, including the derogations in Article 49.

Table of contents

1 Introduction 4

2 What is the scope of these guidelines? 5

3 What is the objective of Article 48? 5

4 In which situations is article 48 applicable? 6

5 Under which conditions can controllers and processors respond to requests from third country authorities? 7

5.1 Compliance with Article 6 GDPR 7

5.2 Compliance with Chapter V GDPR 9

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 "GDPR"),

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. Article 48 GDPR – with the title "Transfers or disclosures not authorised by Union law" – provides that: "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter*".

2. The purpose of these guidelines is to clarify the rationale and objective of Article 48 GDPR, including its interaction with the other provisions of Chapter V of the GDPR, and to provide practical recommendations for controllers and processors in the EU that may receive requests from third country authorities to disclose or transfer[2] personal data.

3. The provision is part of Chapter V of the GDPR on "Transfers of personal data to third countries or international organisations". This means that it has to be read in conjunction with Article 44 GDPR, which clearly states that "***all provisions in this Chapter shall be applied*** *in order to* ***ensure*** *that the* ***level of protection*** *of natural persons guaranteed by [the GDPR]* ***is not undermined***". In addition, Article 48 should be read in conjunction with Recital 102 GDPR, which makes clear that the GDPR "*(...) is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects*".

[1] References to "EU" and "Member States" made throughout this document should be understood as references to "EEA" and "EEA Member States" respectively.

[2] Article 48 refers to "transfers or disclosures". Therefore, this will be the terminology used throughout the text of these guidelines, even though the EDPB made it clear in its Guidelines 05/2021 that a disclosure of personal data qualifies as a transfer provided that the three criteria of the guidelines are met (see part 2.2 of 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).

2 WHAT IS THE SCOPE OF THESE GUIDELINES?

4. These guidelines focus on requests aiming at the direct cooperation between a third country public authority and a private entity in the EU (as opposed to other scenarios where personal data is exchanged directly between public authorities in the EU and in third countries respectively, e.g. on the basis of a mutual legal assistance treaty). Such requests may come from all kinds of public authorities, including those supervising the private sector such as banking regulators and tax authorities, as well as authorities dealing with law enforcement and national security[3].

5. These guidelines only cover the situation where such requests are addressed to controllers or processors in the EU and whose processing of personal data is subject to Article 3.1 of the GDPR.

6. Article 48 does not distinguish between private or public controllers and processors receiving a request for personal data from third country authorities. However, for the purposes of these guidelines, the following analysis focuses on direct requests to private entities in the EU, considering that this appears to be the most common scenario of application of Article 48 and that requests to public authorities usually fall within an international cooperation framework set forth in international agreements.

7. The EDPB highlights that, beyond the requirements of the GDPR, additional rules may govern the cooperation with public authorities in third countries[4]. Such requirements are not addressed in these guidelines.

3 WHAT IS THE OBJECTIVE OF ARTICLE 48?

8. According to Article 48, third country authorities' judgments and decisions requiring a controller or processor in the EU to transfer or disclose personal data may only be recognised and enforced if they are based on an applicable international agreement[5], such as a mutual legal assistance treaty (MLAT) in force between the requesting country and the EU or a Member State[6], without

[3] For the purposes of law enforcement and national security, the exchange of data takes place usually between the authorities involved, so Article 48 is not applicable as these types of transfers do not fall under the scope of the GDPR. The EDPB hence reiterates its position expressed in its guidelines on Article 49 GDPR that: "*In situations where there is an international agreement such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement*". However, there has been a recent tendency to negotiate international agreements to also provide for direct requests from law enforcement authorities in third countries for access to personal data processed by private entities in the EU, e.g. the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

[4] For example, when it comes to cooperation with law enforcement authorities of a third country, criminal procedural rules of the Member State of the entity receiving the request would also apply.

[5] As regards international agreement concluded by the Union, see CJEU Judgment Case C-327/91, French Republic v Commission, para. 27. In relation to Article 228 EEC Treaty, the CJEU notes that Article 228 uses the expression "agreement" in a general sense to indicate any undertaking entered into by entities subject to international law which has binding force, whatever its formal designation.

[6] This wording reflects the international law rules, following which a decision of a national court, tribunal or administrative authority has no legal effect in other jurisdictions unless an applicable international agreement provides for this. Thus, where third country judgments or decisions are directed at entities within the EU, there has to be an international agreement in place between that third country and the EU or the Member State in question in order for those judgments or decisions to be recognised and enforceable under Union or Member State law. However, the need for an international agreement in order for a third country judgment or decision

prejudice to other grounds for transfer pursuant to Chapter V of the GDPR. This article regulates access to personal data subject to the protection of the GDPR by courts and authorities in third countries. Recital 115 clarifies that the provision aims to protect personal data from the extraterritorial application of third country laws which "*may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by the [GDPR]*".

9. Thus, where data processed in the EU are transferred or disclosed in response to a request from a third country authority, such disclosure is subject to the GDPR and constitutes a transfer within the meaning of Chapter V. This means that, as for any transfer subject to the GDPR, there has to be a legal basis for the processing in Article 6 and a ground for transfer in Chapter V.

10. The EDPB reaffirms that a request from a foreign authority does not in itself constitute a legal basis for the processing or a ground for the transfer[7].

4 IN WHICH SITUATIONS IS ARTICLE 48 APPLICABLE?

11. Article 48 applies in situations where a controller or processor in the EU receives a decision or judgment from an administrative authority or a court in a third country requiring the transfer or disclosure of personal data. The wording of the provision, "court", "tribunal" and "administrative authority", refers to a public body in a third country. The EDPB finds that the terminology used by the third country public body to qualify its request as a "decision" or "judgment" is not decisive for the application of Article 48, as long as it is an official request from a third country authority.

12. The EDPB considers that the wording in Article 48 encompasses every possible way in which a controller or processor in the EU could make personal data accessible to a third country authority.

13. Article 48 does not limit the purposes for which data may be requested by the third country authority. Thus, requests from third country authorities issued in different contexts and for different purposes would fall within the scope of the provision e.g. requests from law enforcement or national security authorities, financial regulators or public authorities responsible for approving pharmaceutical products.

14. Article 48 does not distinguish between the situation where a third country authority requests a controller or processor in the EU to transfer or disclose personal data, and the controller or processor can refuse to comply with the request without any adverse legal consequences under EU or third country law and the situation where refusal may lead to sanctions for non-compliance. The EDPB recalls that **in all cases a "two-step test" must be applied** when it comes to any transfer of personal data to third countries*: "first, there must be a legal basis for the data processing together with all relevant provisions of the GDPR; and secondly, the provisions of Chapter V must be complied with. Hence, the processing i.e., the transfer or disclosure of personal data must adhere to the general principles of Article 5 and must rely on a legal basis as stated in Article 6 GDPR*"[8].

to be recognised and enforceable is to be distinguished from the question of whether personal data, also in the absence of such agreement, can be lawfully transferred to a third country.

[7] See to that effect also the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), page 3.

[8] See EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection p. 3. See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

5 UNDER WHICH CONDITIONS CAN CONTROLLERS AND PROCESSORS RESPOND TO REQUESTS FROM THIRD COUNTRY AUTHORITIES?

15. Article 48 is part of Chapter V of the GDPR on 'Transfers of personal data to third countries or international organisations' and has to be read in conjunction with Article 44 GDPR, which states that "*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*". Furthermore, Recital 115 GDPR clarifies that transfers should only be allowed where the conditions of the GDPR are met. This means that any transfer or disclosure of personal data in response to a request from a third country authority requires a legal basis for the processing (Article 6 GDPR) and compliance with the requirements for transfers of personal data to third countries or international organisations (Chapter V GDPR).

16. As already mentioned, in addition to ensuring compliance with the GDPR, a controller or processor may need to comply with additional requirements following from other legal instruments, e.g. national procedural rules or international agreements providing for cooperation with the third country authority.

5.1 Compliance with Article 6 GDPR

17. According to Article 44 GDPR, a transfer of personal data to a third country shall take place only if, subject to the other provisions of the GDPR, the conditions of Chapter V are complied with. Therefore, transferring personal data to third countries or international organisations must also meet the conditions of the other provisions of the GDPR.

18. Article 5(1) of the GDPR sets out general and mandatory principles for the processing of personal data. According to Article 5(2), the controller is responsible for compliance with the obligations set out in paragraph 1 (this applies as well when the processing activities are carried out by means of a processor). According to Article 5(1), any processing of personal data must have a legal basis under Article 6. A legal analysis is therefore required with regard to each specific situation.

19. The case described in Article 48 presupposes that there is a judgement of a court or tribunal or a decision of an administrative authority of a third country that requires a controller or processor in the EU to transfer or disclose personal data. Furthermore, this request from a third country authority may only be recognised or made enforceable if it is based on an international agreement, which may give such request the effect of a legal obligation to which the controller is subject and non-compliance would have legal consequences. Where the processing of personal data is carried out in order to fulfil a legal obligation, **Article 6(1)(c)** provides an explicit legal basis. As a result, the EDPB is of the opinion that for the case outlined in Article 48, where there is an applicable international agreement in place, Article 6(1)(c) in conjunction with Article 6(3) would be the appropriate legal basis for the transfer provided that the conditions of these provisions are fulfilled.

20. In cases where there is no legal obligation arising from an international agreement for the controller, the use of other legal bases under Article 6 remains possible, provided that the legal requirements set out by Chapter V of the GDPR are fulfilled. However, the application of these other legal bases must be carefully examined on a case-by-case basis. Due to the large number of

possible situations, general statements on the applicability of Article 6 can only be made to a very limited extent.

21. In principle, consent pursuant to Article 6(1)(a) could be considered as a legal basis for a transfer to third countries. However, the use of consent as a legal basis will usually be inappropriate in certain areas, especially if the processing of the data is related to the exercise of authoritative powers[9].

22. The application of Article 6(1)(b) appears to be excluded by its wording alone. The EDPB is therefore of the view that Article **6(1)(b) cannot be relied upon** by a private entity in the EU as an appropriate legal basis to answer a request for transfer or disclosure from a third country authority.

23. In situations where disclosure based on an international agreement is not mandatory, but such cooperation is still permitted under EU or Member State law, **Article 6(1)(e)** could be used as a legal basis for the processing of personal data since it can be considered necessary for the performance of the task carried out in the public interest[10]. In such cases, the processing has to have a basis in Union or Member State law as required in Article 6(3) GDPR.

24. As for **Article 6(1)(d)**, the EDPB recognises that in specific and established circumstances, the **vital interests of the data subject** could be cited as a legal basis for a transfer of personal data triggered by a third country request provided that the conditions set out in international law are met[11]. With regards to the **vital interest of other persons** the EDPB recalls that "*processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis*" [12].

25. Depending on the individual case, the EDPB assumes that it may be possible to rely on **Article 6(1)(f)** for transfers or disclosures to third country authorities[13] in exceptional circumstances. To this effect, the EDPB recalls that any processing based on the legitimate interests of the controller or third parties must be necessary and balanced against the interests or fundamental rights and freedoms of the data subject[14]. The outcome of the balancing test determines whether the legal basis of legitimate interest may be relied upon for the processing.

[9] See in this context the legal concept of recital 43 s. 1 concerning the requirement of freely given consent. This applies all the more if the case related to public bodies from third countries. See also EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, footnote 28.

[10] See for example Article 6 of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

[11] This could for instance be the case of requests to access personal data concerning abducted minors or other situations where the transfer is in the vital interest of data subjects themselves.

[12] Recital 46 GDPR.

[13] For further information see EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (version 1.0) adopted on 8 October 2024.

[14] Assessing the impact on the data subject's interests shall take into account any possible (potential or actual) consequences of the data processing for the data subject, the data protection principles of proportionality, as well as elements such as, for example, the seriousness of the alleged offences that may be notified, the scope of the request, applicable standards and procedural guarantees in the third country, and applicable data protection safeguards. Such assessment shall also pay particular attention to the nature of the personal data processed and the way personal data are being processed. In addition, the GDPR also introduced the necessity to take into account the reasonable expectations of the data subject. For further information on the necessity and balancing test see also EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (version 1.0) adopted on 8 October 2024.

In principle, any processing based on legitimate interest is in any case limited to what is demonstrably necessary to pursue this specific interest of the controller or the third party.

26. Despite the fact that a controller, in some cases, may have a legitimate interest to comply with a request to disclose personal data to a third country authority, a private business operator, acting as controller, cannot rely on Article 6(1)(f) for the collection and storing of personal data in a preventive manner in order to be able to share such information, upon request, with law enforcement authorities so as to prevent, detect and prosecute criminal offences, where such processing activities are unrelated to its own actual (economic and commercial) activities[15]. Moreover, the EDPB has, with respect to a specific situation, previously taken the view that the interests or fundamental rights and freedoms of the data subject in those particular circumstances would override the controller's interest of adhering to the request of a third country law enforcement authority in order to avoid sanctions for non-compliance[16].

5.2 Compliance with Chapter V GDPR

27. As already stated above, Article 48 must be read in conjunction with Article 44, the general principle for transfers introducing the chapter. Article 44 lays down the following conditions for transfers under the GDPR: any transfer is subject to the other relevant provisions of the GDPR and complies with the conditions laid down in Chapter V (the two-step test), *"in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined*". The provisions on international transfers are designed to ensure that the high level of protection for personal data within the EU/EEA is upheld when data are transferred to third countries with different legal systems and data protection standards.

28. For this purpose, Chapter V lists the grounds for transfers, starting with the European Commission's adequacy decisions under Article 45. If there is no adequacy decision, appropriate safeguards may be provided for by one of the transfer tools foreseen in Article 46. In the absence of an adequacy decision or appropriate safeguards, the derogations in Article 49 could apply in a limited number of specific situations.

29. Unlike the other provisions of Chapter V, Article 48 is not a ground for transfer. The provision itself contains no data protection safeguards but clarifies that decisions or judgments from third country authorities cannot be recognised or enforced in the EU/EEA unless an international agreement provides for this. Therefore, before responding to a request from a third country authority falling under Article 48, the controller or processor in the EU/EEA must identify an applicable ground for the transfer elsewhere in Chapter V.

30. According to Article 46(2)(a) appropriate safeguards may be provided for by "*a legally binding and enforceable instrument between public authorities or bodies*" i.e. an international agreement within the meaning of Article 48. Such agreements are concluded by states and traditionally allow for cooperation between public authorities, but may also provide for direct cooperation between private entities and public authorities[17]. If an international agreement covers the cooperation

[15] Judgment of the Court (Grand Chamber) of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, Case C-252/21, para. 124 and 132.
[16] See EDPB position already expressed for the area of law enforcement and national security in the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection.
[17] See as an example Council of Europe: Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

between the controller or processor in the EU/EEA and the requesting third country authority, this agreement may serve as a ground for transfer if it provides for the appropriate safeguards in accordance with Article 46(2)(a).

31. The EDPB has elaborated a list of minimum safeguards to be included in international agreements falling under Article 46(2)(a). Such safeguards must be capable of ensuring that data subjects whose personal data are transferred are afforded a level of protection essentially equivalent to that, which is guaranteed within the EU/EEA[18]. Consequently, international agreements providing for transfers of personal data should *inter alia* require that the core data protection principles are guaranteed by both parties, i.e. ensuring enforceable and effective data subject rights, containing restrictions on onward transfers and data sharing, including additional safeguards for sensitive data and providing independent redress and supervision mechanisms[19]. The appropriate safeguards may be included directly in the international agreement, which provides for the direct cooperation between the controller or processor and the third country authorities, or in a separate legally binding instrument.

32. Article 48 refers to an international agreement "*without prejudice to other grounds for transfer pursuant to this Chapter*". In the opinion of the EDPB, with regard to Chapter V requirements[20], this wording might cover two possible situations:
    - First, if there is **no international agreement** providing for cooperation between the controller or processor and the third country authority, a transfer to a third country authority must be based on another legal basis under Article 6 GDPR and another ground for transfer in Chapter V.
    - Second, if there is an international agreement providing for the legal basis under Article 6, but **it does not contain the appropriate safeguards** in accordance with Article 46(2)(a) and the EDPB Guidelines 2/2020, the controller must identify another ground for transfer in Chapter V.

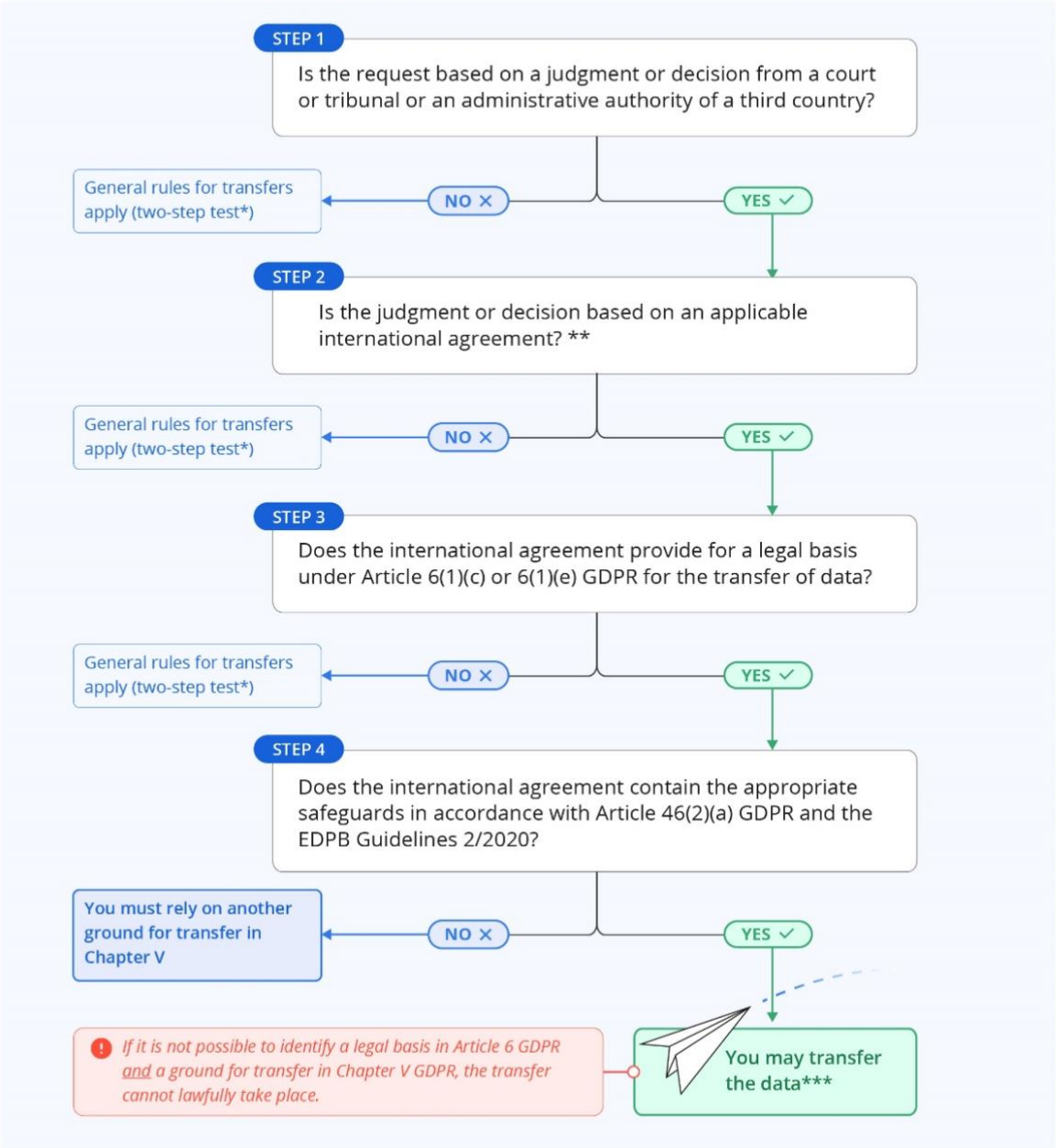
33. In the absence of an applicable adequacy decision[21] or appropriate safeguards, Article 49 GDPR offers a limited number of specific situations in which transfers may take place, for instance if they are necessary for important reasons of public interest or for the establishment to exercise or defence of legal claims[22]. However, as explained in previous guidance issued by the EDPB, the derogations in Article 49 GDPR must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive[23].

[18] Court of Justice of the European Union, Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), para. 96.
[19] See in this regard part 2 of 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, version 2.0; adopted on 15 December 2020.
[20] With regard to Article 6 GDPR, there could be a third situation where there is an international agreement in place that does not provide an appropriate legal basis under Articles 6(1)(c) or 6(1)(e) GDPR, for instance because the relevant provisions of the agreement are not specific enough (e.g. they do not reflect the elements listed in Article 6(3) GDPR).
[21] The assessment whether an adequacy decision is applicable should be done on a case by case basis, taking in particular into account the scope of the adequacy decision.
[22] See Article 49(1)(d) and (e) GDPR.
[23] See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 adopted on 25 May 2018.

Annex - Practical steps

Article 48 refers to the situation where a public body in a third country requests a controller or processor in the EU to transfer data to that authority and the request stems from a judgment or decision of a court or tribunal or an administrative authority of the third country.

When receiving a **request** for personal data from an authority in a third country, a controller or processor in the Union should answer the following questions in order to decide if the request can be complied with:



*Two-step test: A lawful transfer requires a legal basis in Article 6 GDPR and a ground for transfer in Chapter V GDPR.
** In this particular situation, an applicable international agreement would mean an international agreement providing for the possibility of direct requests from public authorities in third countries for access to personal data processed by private entities in the EU. If there is no such agreement but an international agreement provides for cooperation between public authorities in that specific area, such as a mutual legal assistance treaty (MLAT), private entities in the EU should generally refer the requesting third country authority to its national competent authority, in line with the procedure provided by the MLAT or agreement (see also footnote 3 of the guidelines).
***Provided that compliance with the other relevant provisions of the GDPR is ensured.