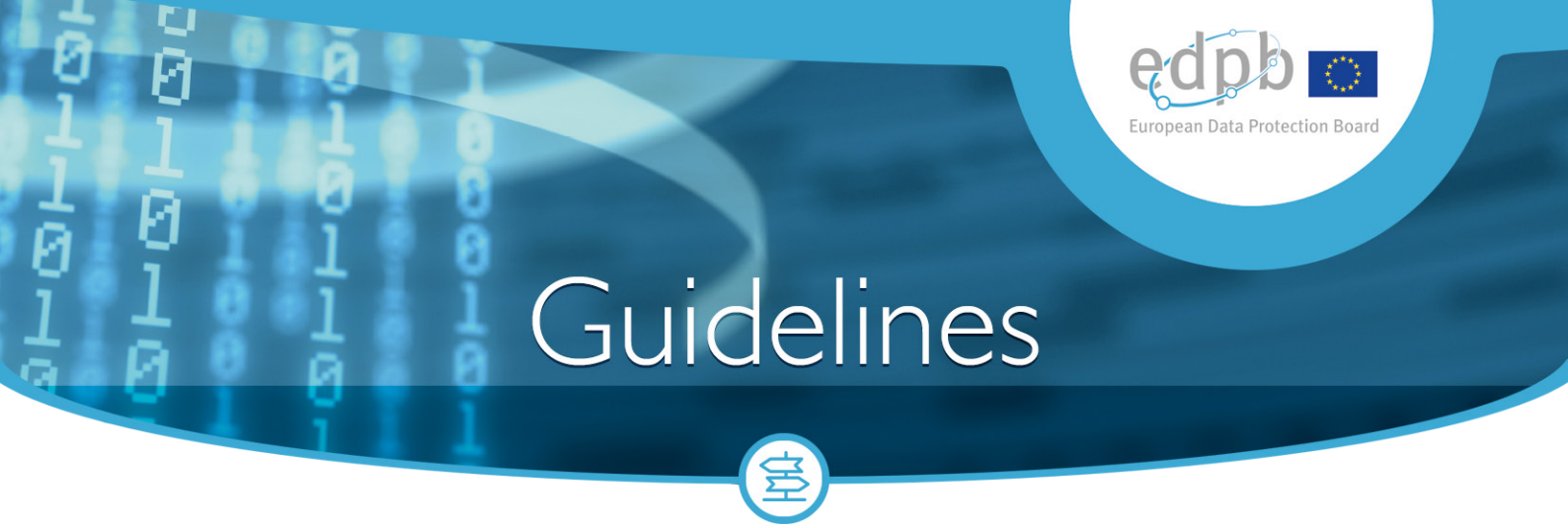


Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Version 2.0

Adopted on 14 February 2023

Version history

Version 2.0	14 02 2023	Adoption of the Guidelines after public consultation
Version 1.0	18 11 2021	Adoption of the Guidelines for public consultation

EXECUTIVE SUMMARY

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". Therefore, the EDPB provides these guidelines to clarify the scenarios to which it considers that the requirements of Chapter V should be applied and, to that end, it has identified three cumulative criteria to qualify a processing operation as a transfer:

1) A controller or a processor ("exporter") is subject to the GDPR for the given processing.
2) The 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, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.

If the three criteria as identified by the EDPB are met, there is a transfer and Chapter V of the GDPR is applicable. This means that the transfer can only take place under certain conditions, such as in the context of an adequacy decision from the European Commission (Article 45) or by providing appropriate safeguards (Article 46). 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.

Conversely, if the three criteria are not met, there is no transfer and Chapter V of the GDPR does not apply. In this context, it is however important to recall that the controller must nevertheless comply with the other provisions of the GDPR and remains fully accountable for its processing activities, regardless of where they take place. Indeed, although a certain data transmission may not qualify as a transfer according to Chapter V, such processing can still be associated with increased risks since it takes place outside the EU, for example due to conflicting national laws or disproportionate government access in the third country. These risks need to be considered when taking measures under, *inter alia*, Article 5 ("Principles relating to processing of personal data"), Article 24 ("Responsibility of the controller") and Article 32 ("Security of processing") – in order for such processing operation to be lawful under the GDPR.

These guidelines include various examples of data flows to third countries, which are also illustrated in an Annex in order to provide further practical guidance.

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 44 of 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 therefore 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 in the EU, it is protected not only by the rules in the GDPR but also by other rules, both at 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 transmitted or made available to entities outside the EU territory or to international organisations, the level of protection of individuals' rights and freedoms is likely not to be essentially equivalent to the one afforded by the the overarching legal framework provided within the Union.

3. Continuity of protection can be ensured in different ways, such as by the legal framework of a third country or international organisation that benefits from an adequacy decision from the European Commission (Article 45) or by an instrument between the data exporter and importer providing for

[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."

appropriate safeguards (Article 46).[5] When relying on one of the transfer instruments listed in Article 46 GDPR, it must be assessed whether they ensure a level of protection of the transferred data that is essentially equivalent to that guaranteed within the EU or whether supplementary measures need to be implemented.[6]

4. Where a controller or processor transfers data to an importer in a third country whose processing falls under Article 3(2) of the GDPR, the protection provided by the GDPR may similarly be undermined by the legal framework that applies to the importer. 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.

5. The following sections aim at clarifying this interplay between Article 3 and the provisions of the GDPR on international transfers in Chapter V. The purpose is to assist controllers and processors with identifying whether a processing operation 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. This clarification is also important for the consistent interpretation and application of the GDPR by the supervisory authorities.

6. In any event, and as explained in more detail in Section 4, it is important to keep in mind that although a certain data flow subject to Article 3 may not always constitute a transfer under Chapter V, the processing of data outside the EU can still be associated with increased risks for which safeguards must be envisaged. Regardless of whether the processing takes place in the EU or not, controllers and processors subject to the GDPR for a given processing always have to comply with all relevant provisions of the GDPR, such as the Article 32 obligation to implement technical and organisational measures taking into account, *inter alia*, the risks with respect to the processing.

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

7. 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"[7] and relevant case law is limited.[8] The lack of definition of transfer in the GDPR leads to legal uncertainty about the precise scope of the obligations deriving from

[5] When the continuity of protection cannot be ensured by the transfer instrument used, for example if an adequacy decision under Article 45 is revoked, a certification mechanism under Article 46(2)(f) is no longer valid or adopted supplementary measures are not/no longer effective, measures must be taken in order to avoid that the level of protection is undermined and to ensure that the processing in question is lawful, e.g. another transfer tool and/or effective supplementary measures must be put in place.

[6] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures and CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, EU:C:2020:559.

[7] Article 44, sentence 1.

[8] Such as the CJEU Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596 according to which a transfer is a processing operation and there is no transfer to a third country, under the former Directive 95/46, where data is published on a website stored with a hosting provider established in the EU.

Chapter V and the interplay between Article 3 and Chapter V. It is therefore essential to clarify this notion.

8. Considering that the EDPB, according to Article 70(1)(b) GDPR, has the task to advise the European Commission on any issue related to the protection of personal data in the Union, including on any aspects of the Regulation that it considers to require further clarification, the EDPB invites the European Commission to pay particular attention to this issue in the context of the report on the evaluation and review of the GDPR as per Article 97.

9. In any event, considering that Article 70(1)(e) GDPR sets forth the task for the EDPB to issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation, the EDPB provides this guidance to clarify the scenarios to which it considers that the requirements of Chapter V should be applied. To that end, it has identified the following three cumulative criteria to qualify a processing operation as a transfer:

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

    2) The 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, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.

10. In this respect, it is important to recall that, pursuant to Article 3, whether or not the GDPR applies must always be assessed in relation to a certain processing operation rather than with regard to a specific entity (e.g. a company).[9]

11. The EDPB also recalls 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 (regardless of where they are located).[10]

2.1 A controller or a processor ("exporter") is subject to the GDPR for the given processing

12. 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).

13. 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 controller or processor in the same or another third country or to an international organisation, taking into account that the obligations under the GDPR are not different for controllers/processors established in the EU and controllers/processors outside the EU whose processing falls under Article 3(2).

[9] See page 5 and Sections 1–3 of the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).
[10] Idem, see page 23.

14. It can also be noted that the GDPR, including Chapter V, applies to personal data processing carried out by EU Member States' embassies and consulates located outside the EU as such processing falls within the scope of the GDPR by virtue of Article 3(3).[11]

2.2 The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer")

15. The second criterion requires that the exporter discloses data by transmission or otherwise makes it available to another controller or processor. The concepts of controller and processor have been further clarified in the EDPB Guidelines 07/2020. It should 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.[12]

16. Some examples of how personal data could be "made available" are by creating an account, granting access rights to an existing account, "confirming"/"accepting" an effective request for remote access, embedding a hard drive or submitting a password to a file. It should be kept in mind that remote access from a third country (even if it takes place only by means of displaying personal data on a screen, for example in support situations, troubleshooting or for administration purposes) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer, provided that the three criteria outlined in paragraph 9 above are met.[13]

17. Conversely, Chapter V does not apply to "internal processing", i.e. where data is not disclosed by transmission or otherwise made available to another controller or processor, including where such processing takes place outside the EU.[14] In this case, the controller or processor remains responsible for the processing, including to ensure compliance with all relevant provisions and safeguards of the GDPR which directly applies (see also Section 4 below), e.g. the EEA supervisory authorities can enforce the GDPR against these entities and data subjects can obtain redress in case of a violation of their rights.

18. In addition, this second criterion cannot be considered as fulfilled when there is no controller or processor sending or making the data available (i.e. no "exporter") to another controller or processor, such as when data are disclosed directly by the data subject[15] to the recipient.

---

[11] Idem, see page 22.

[12] See page 9 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[13] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, page 11, paragraph 13 and footnote 28.

[14] This is also reflected in the approach of Article 46 GDPR, which refers to contractual/bilateral transfer instruments concluded between different entities acting as controllers or processors.

[15] 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 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. 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. Finally, it should be noted

Example 1: Controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR)

Maria, living in Italy, inserts her name, surname and postal address by filling in 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 third country company that has no presence in the EU, but specifically targets the EU market. In this case, the data subject (Maria) passes her personal data to the third country company. This does not constitute a transfer of personal data since the data are not passed by an exporter (controller or processor), but directly collected from the data subject by the controller under Article 3(2) GDPR. Thus, Chapter V does not apply to this case. Nevertheless, the third country company will be required to apply the GDPR since its processing operations are subject to Article 3(2).[16]

Example 2: Controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities

Maria, living in Italy, inserts her name, surname and postal address by filling in 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 third country company that has no presence in the EU, but specifically targets the EU market. In order to process the orders received by means of the website, the third country company has engaged a non-EEA processor. In this case, the data subject (Maria) passes her personal data to the third country company and this does not constitute a transfer of personal data since the data are directly collected by the controller under Article 3(2) GDPR. Thus, the controller will have to apply the GDPR to the processing of this personal data. As far as it engages a non-EEA processor, such disclosure from the third country company to its non-EEA processor would amount to a transfer, and it will be required to apply Article 28 and Chapter V obligations so as to ensure that the level of protection afforded by the GDPR would not be undermined when data are processed on its behalf by the non-EEA-processor.[17]

Example 3: Controller in a third country receives data directly from a data subject in the EU (but not under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities

Maria, living in Italy, decides to book a room in a hotel in New York using a form on the hotel website. Personal data are collected directly by the hotel which does not target/monitor individuals in the EEA. In this case, no transfer takes place since data are passed directly by the data subject and directly collected by the controller. Also, since no targeting or monitoring activities of individuals in the EEA are taking place by the hotel, the GDPR will not apply, including with regard to any processing activities carried out by non-EEA processors on behalf of the hotel.

---

that personal data disclosed via cookies are not considered as being disclosed directly by the data subject, but rather as a transmission by the operator of the website that the data subject is visiting.

[16] 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.

[17] Note that when the processing activities by the processor are related to the targeting activities of the controller, the processor is also subject to Article 3(2) of the GDPR, see page 20–22 of the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

Example 4: Data collected by an EEA platform and then passed to a third country controller

Maria, living in Italy, books a room in a hotel in New York by means of an online EEA travel agency. Maria's personal data, necessary for booking the hotel, are collected by the EEA online travel agency as a controller and sent to the hotel receiving the data as a separate controller. While passing the personal data to the third country hotel, the EEA travel agency carries out a transfer of personal data and Chapter V GDPR applies.

Example 5: 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 Company Z in a third country, which processes these data as processor on behalf of Company 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.

19. 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 will be a transfer situation where a processor (either under Article 3(1) or under Article 3(2) for a given processing, as explained above) sends data to another processor or even to a controller in a third country as instructed by its controller.[18] In these cases, the processor acts as a data exporter on behalf of the controller and has to ensure that the provisions of Chapter V are complied with for the transfer at stake according to the instructions of the controller, including that an appropriate transfer tool is used. Considering that the transfer is a processing activity carried out on behalf of the controller, the controller is also responsible and could be liable under Chapter V, and also has to ensure that the processor provides for sufficient guarantees under Article 28.

Example 6: 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 data subjects not located in the EU, 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 7: 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 in a third country, and hence to send the data for

[18] Article 28(3)(a) GDPR refers to the documented instructions from the controller "including with regard to transfers of personal data to a third country or an international organisation". See also Clause 8.1 of Module three in Annex to the 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.

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.

20. As mentioned in paragraph 17 above, 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 8: 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 a third country for a meeting bringing his laptop. During his stay abroad, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This bringing of the laptop and remote access of personal data from a third country, does not qualify as a transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (A).[19] Therefore, the transmission 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. It can, however, be noted that in case George, in his capacity as an employee of A, would send or make data available to another controller or processor in the third country, the data flow in question would amount to a transfer under Chapter V; from the exporter (A) in the EU to such importer in the third country.

21. 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.[20]

Example 9: A subsidiary (controller) in the EU shares data with its parent company (processor) in a third country

The Irish Company X, which is a subsidiary of the parent Company Y in a third country, discloses personal data of its employees to Company Y to be stored in a centralised HR database by the parent company in the third country. In this case the Irish Company X processes (and discloses) the data in its capacity of employer and hence as a controller, while the parent company is a processor. Company X is subject to the GDPR pursuant to Article 3(1) for this processing and Company Y 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.

2.3 The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation

[19] See paragraph 78 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[20] As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment may be acting as a controller or processor, e.g. when processing data on behalf of the parent company, see paragraph 17 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

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

23. The EDPB highlights that this criterion is aimed at ensuring that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data are no longer processed within the EEA legal framework (see, in this respect, the last sentence of Article 44 and Recital 101 GDPR). This may happen either because the GDPR does not apply to the importer for the given processing or because personal data, even if the given processing is subject to the GDPR,[21] are processed by an importer located outside the EEA and therefore could be subject to different (conflicting) legal frameworks, e.g. as regards possible disproportionate government access to personal data. In this context, possible difficulties to enforce compliance with the GDPR and to obtain redress against entities located outside the EEA are also relevant considerations.

Example 10: 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.

Example 11: Remote access to data in the EU by a third country processor acting on behalf of EU controllers

A company in a third country (Company Z), with no establishment in the EU, offers services as a processor to companies in the EU. Company Z, acting as processor on behalf of the EU controllers, is remotely accessing, e.g. for support purposes, the data which is stored in the EU. Since Company Z is located in a third country, such remote access results in transfers of data from the EU controllers to their processor (Company Z) in a third country under Chapter V.

24. Another situation worth mentioning in this context is when a controller in the EU uses a processor in the EU subject to third country legislation and there is a possibility that the processor will receive government access requests and, thus, a transfer of personal data will take place if the processor acts on such request. In such situation, it should be kept in mind that according to Article 28(1) and Recital 81 GDPR, controllers may only use processors that provide sufficient guarantees that technical and organisational measures are taken that meet the requirements of the GDPR. In this context, the GDPR does not only refer to expertise and resources but also to reliability, which may be in doubt if the processor is subject to third country legislation which may prevent it from fulfilling its obligations as a processor. The question of whether the processor provides sufficient guarantees also concerns the lawfulness of the processing and the respect of the principle of integrity and confidentiality for which the controller is accountable under Article 5(2) of the GDPR.[22]

[21] As mentioned above, whether the processing in question meets the requirements of Article 3 GDPR, i.e. that the importer is subject to the GDPR for the given processing, has been further elaborated on in the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

[22] See also paragraphs 119–120 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Example 12: Controller in the EU uses a processor in the EU subject to third country legislation

The Danish Company X, acting as controller, engages Company Y established in the EU as a processor on its behalf. Company Y is a subsidiary of the third country parent Company Z. Company Y is processing the data of Company X exclusively in the EU and there is no one outside the EU, including the parent Company Z, who has access to the data. Additionally, it follows from the contract between Company X and Company Y that Company Y shall only process the personal data on documented instructions from Company X, unless required to do so by EU or Member State law to which Company Y is subject. Company Y is however subject to third country legislation with extraterritorial effect, which in this case means that Company Y may receive access requests from third country authorities. Since Company Y is not in a third country (but an EU company subject to Article 3(1) GDPR), the disclosure of data from the controller Company X to the processor Company Y does not amount to a transfer and Chapter V of the GDPR does not apply. As mentioned, there is however a possibility that Company Y receives access requests from third country authorities and should Company Y comply with such request, such disclosure of data would be considered a transfer under Chapter V. Where Company Y complies with a request in violation of the controller's instructions and thus Article 28 GDPR, Company Y shall be considered an independent controller of that processing under Article 28(10) GDPR. In this situation, the controller Company X should, before engaging the processor, assess these circumstances in order to ensure that, as required by Article 28 GDPR, it only uses processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing is in line with the GDPR, including Chapter V, as well as to ensure that there is a contract or legal act governing the processing by the processor.

3 CONSEQUENCES IN CASE A TRANSFER OF PERSONAL DATA TAKES PLACE

25. 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, or to an international organisation.

26. As a consequence, the exporter needs to comply with the conditions of Chapter V and frame the transfer by using one of the instruments that aim at protecting personal data after they have been transferred to a third country or an international organisation.

27. These instruments include an adequacy decision adopted by the European Commission recognising 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.[23] In addition, 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 in specific situations and under certain conditions.[24]

[23] 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.
[24] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

28. The main types of transfer instruments listed in Article 46 are:

- Standard Contractual Clauses (SCCs);
- Binding Corporate Rules (BCRs);
- Codes of conduct;[25]
- Certification mechanisms;[26]
- Ad hoc contractual clauses;
- International agreements/Administrative arrangements.[27]

29. The content of the safeguards provided for by the transfer instruments needs to be adapted 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 ones to be provided for a transfer by a controller.[28] Similarly, for a transfer of personal data to a controller or processor in a third country who is already subject to the GDPR for the given processing, it has to be noted that the GDPR already applies in its entirety. Therefore, for such scenario, when developing relevant transfer instruments under Article 46, namely standard contractual clauses[29] or ad hoc contractual clauses,[30] the Article 3 situation should be taken into account in order not to duplicate the GDPR obligations but rather to address the elements that are related specifically to the risks associated with the importer being located in a third country, e.g. to address possible 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. Such instruments 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 requests for disclosure of data. The EDPB encourages and stands ready to cooperate in the development of a transfer instrument, such as a new set of standard contractual clauses pursuant to Article 46(2)(c), in cases where the importer is subject to the GDPR for the given processing. The EDPB takes note that the European Commission has indicated that it is in the process of developing an additional set of standard contractual clauses for this scenario

[25] EDPB has adopted Guidelines 04/2021 on Codes of Conduct as tools for transfers.
[26] EDPB has adopted Guidelines 07/2022 on Certification as a tool for transfers.
[27] EDPB has adopted 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.
[28] See e.g. the different safeguards in Module 1 and Module 3 of Annex to the 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 (the "Implementing Decision").
[29] The standard contractual clauses (SCCs) adopted by the European Commission on 4 June 2021, according to Article 1 of the Implementing Decision, provide appropriate safeguards for transfers from exporters of personal data subject to the GDPR to importers whose processing of the data is *not subject to the GDPR*. Note that this concerns the scope of application of the SCCs and does not interpret the notion of transfer under Chapter V of the GDPR.
[30] Note that according to Article 40(3), codes of conduct may be adhered to by controllers or processors that are *not subject to the GDPR* in order to provide appropriate safeguards under Article 46(2)(e). Similarly, pursuant to Article 42(2), certification mechanisms, seals or marks may be established in order to demonstrate the existence of appropriate safeguards under Article 46(2)(f) provided by controllers or processors that are *not subject to the GDPR*. This is why the EDPB, currently, has identified SCCs and ad hoc clauses as the available and most relevant transfer tools for data flows to importers subject to the GDPR. This notwithstanding, code of conducts and certifications play important roles as tools for controllers and processors to ensure and demonstrate compliance with the GDPR in relation to processing operations falling under the GDPR according to Article 3. As such, the adherence to both types of instruments may be taken into account when personal data are transferred to a controller or a processor in a third country subject to the GDPR.

which will take into account the requirements that already apply directly to those controllers and processors under the GDPR.[31]

30. Conversely, if the criteria as identified by the EDPB are not met, there is no transfer and Chapter V of the GDPR does not apply.

4 SAFEGUARDS TO BE PROVIDED IF PERSONAL DATA ARE PROCESSED OUTSIDE THE EEA BUT NO TRANSFER TAKES PLACE

31. In light of the criteria identified above, if the same controller or processor is processing data outside the EU without disclosing it to another controller or processor (e.g. where an employee of an EU controller travels abroad and has access to the data of that controller while being in a third country or in case of direct collection from individuals in the EU under Article 3(2) GDPR), the processing activity should not be regarded as a transfer under Chapter V of the GDPR. In this context, it should however be kept in mind that the controller must comply with the GDPR and remains accountable for its processing activities, regardless of where they take place. This also means that the controller or processor should pay particular attention to the legal frameworks of the third country that may have an impact on its ability to respect the GDPR. Indeed, although a certain data transmission may not qualify as a transfer to a third country in accordance with Chapter V of the GDPR, including the scenario described in Example 8, such processing can still be associated with increased risks because it takes place outside the EU, for example due to conflicting national laws or disproportionate government access in a third country. These risks must be considered when taking measures to ensure compliance with the GDPR, including under Article 5 ("Principles relating to processing of personal data"), 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.

32. Following from its obligation to be responsible for, and be able to demonstrate compliance with the data protection principles (Article 5) and 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. In a transfer situation, once an essentially equivalent level of protection cannot be guaranteed, the CJEU ultimately demands the transfer to be suspended or stopped.[32] In this regard, the Court focuses on the risks that a specific processing operation entails due to its cross-border dimension. These requirements are also of relevance when assessing situations that hold similar risks (although not considered as transfers),[33] e.g. in relation to disproportionate government access by third country authorities. For example, a controller may conclude that employees cannot bring their laptops etc. to certain third countries. In this context, and as mentioned above, it should be underlined that as soon as the data are disclosed by transmission or otherwise made available to

[31] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en).
[32] Cf. CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, EU:C:2020:559, paragraph 135.
[33] It can be noted that the adequacy status of a certain third country would also be of relevance in such assessment.

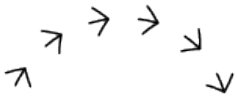
another controller or processor (also being a public authority) in the third country (for example by an employee on a business trip), the data flow in question would amount to a transfer under Chapter V.

33. Moreover, when a controller intends to process personal data outside the EU (although no transfer takes place), this information should as a rule be provided to individuals as part of the controller's transparency obligations, e.g. to ensure compliance with the principle of transparency and fairness, which also requires controllers to inform individuals of the risks in relation to the processing.[34]

34. To summarize, controllers and processors whose processing is subject to the GDPR are responsible for all their processing activities, regardless of where they take place, and data processing in third countries may involve increased risks, including in relation to disproportionate government access, which need to be identified and attentively addressed in order for such processing to be lawful under the GDPR. The EDPB will assess the need for additional guidance to be issued on safeguards in this regard.

[34] See Recitals 39 and 60 GDPR and the WP29 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), paragraph 10.

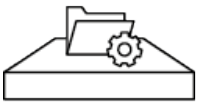
ANNEX: ILLUSTRATIONS OF EXAMPLES 1–12



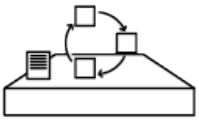
Data flow
Not considered as data transfer

Data transfer
Chapter V GDPR

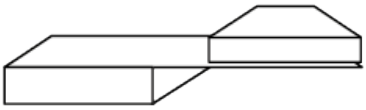
GDPR Articles and Chapters



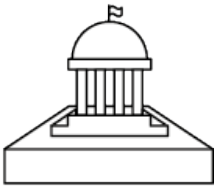
Controller



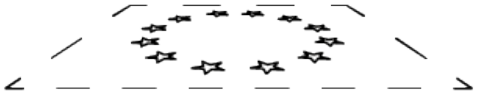
Processor



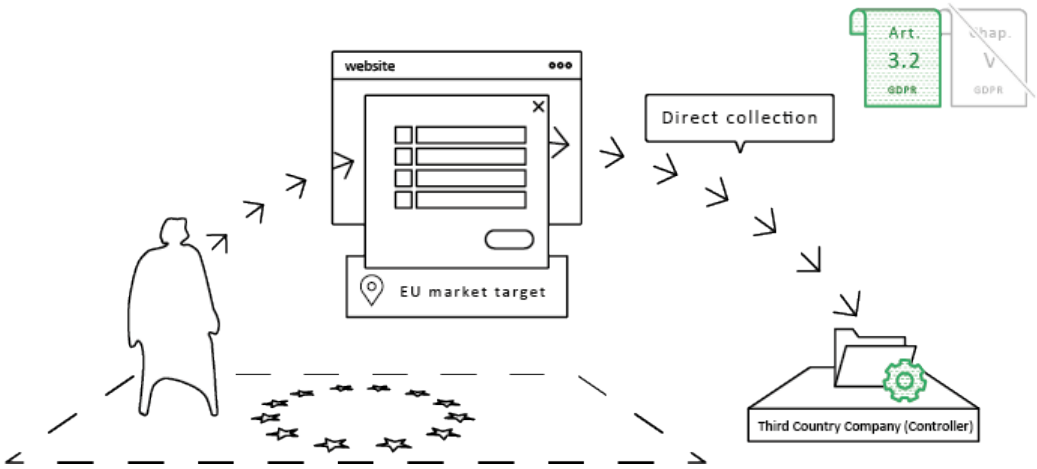
Parent company and subsidiary company



Third country authority

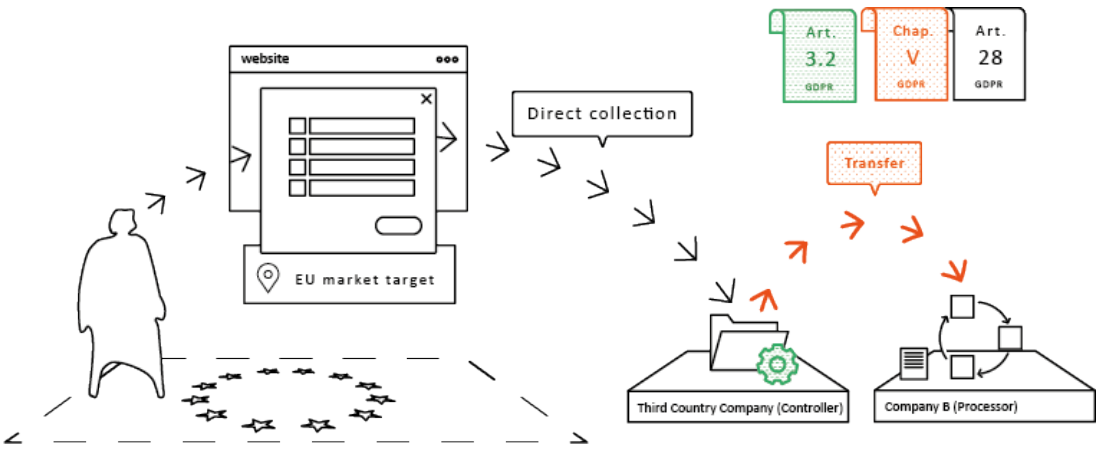


EU / EEA area and limits



Example 1: Controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR)

Maria, living in Italy, inserts her name, surname and postal address 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 third country company that has no presence in the EU, but specifically targets the EU market. In this case, the data subject (Maria) passes her personal data to the third country company. This does not constitute a transfer of personal data since the data are not passed by an exporter (controller or processor), but directly collected from the data subject by the controller under Article 3(2) GDPR. Thus, Chapter V does not apply to this case. Nevertheless, the third country company will be required to apply the GDPR since its processing operations are subject to Article 3(2).

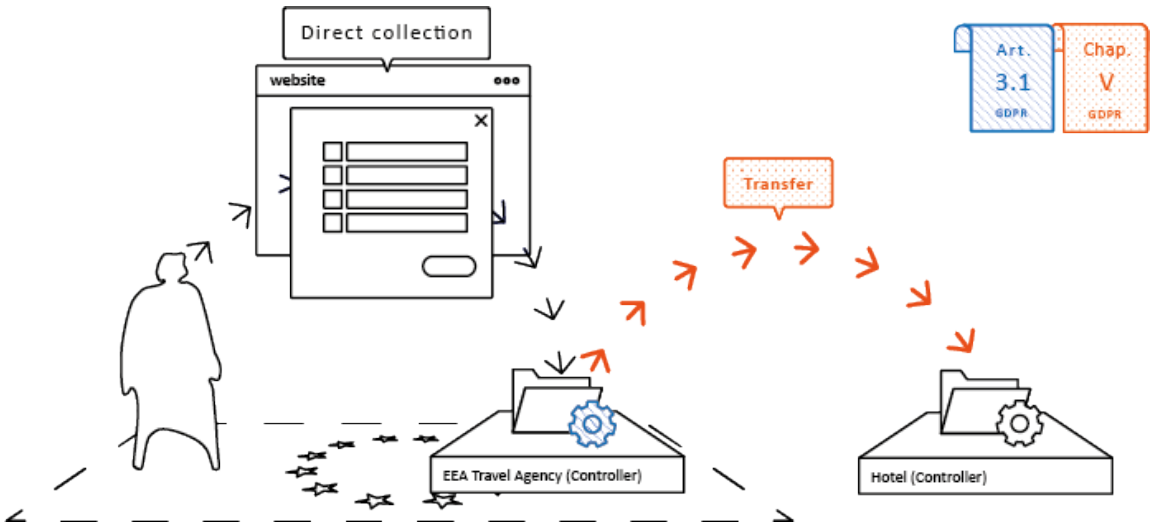


Example 2: Controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities

Maria, living in Italy, inserts her name, surname and postal address 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 third country company that has no presence in the EU, but specifically targets the EU market. In order to process the orders received by means of the website, the third country company has engaged a non-EEA processor. In this case, the data subject (Maria) passes her personal data to the third country company and this does not constitute a transfer of personal data since the data are directly collected by the controller under Article 3(2) GDPR. Thus, the controller will have to apply the GDPR to the processing of this personal data. As far as it engages a non-EEA processor, such disclosure from the third country company to its non-EEA processor would amount to a transfer, and it will be required to apply Article 28 and Chapter V obligations so as to ensure that the level of protection afforded by the GDPR would not be undermined when data are processed on its behalf by the non-EEA-processor.

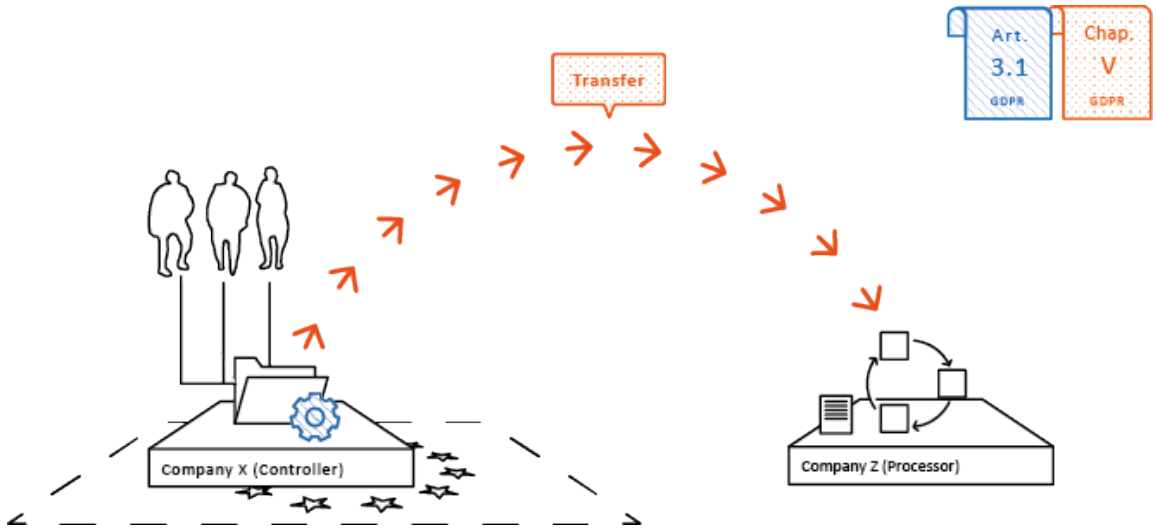
Example 3: Controller in a third country receives data directly from a data subject in the EU (but not under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities

Maria, living in Italy, decides to book a room in a hotel in New York using a form on the hotel website. Personal data are collected directly by the hotel which does not target/monitor individuals in the EEA. In this case, no transfer takes place since data are passed directly by the data subject and directly collected by the controller. Also, since no targeting or monitoring activities of individuals in the EEA are taking place by the hotel, the GDPR will not apply, including with regard to any processing activities carried out by non-EEA processors on behalf of the hotel.



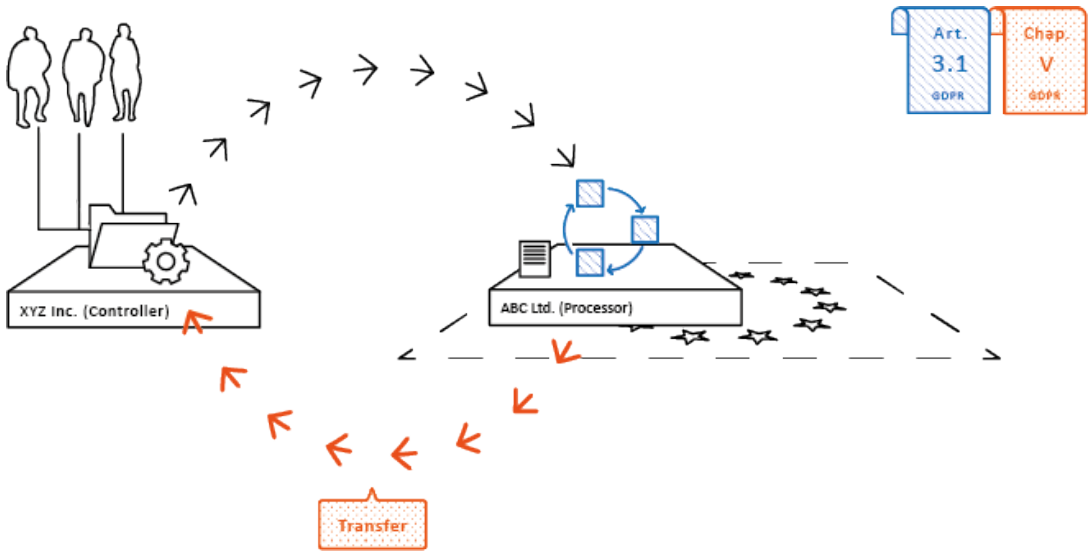
Example 4: Data collected by an EEA platform and then passed to a third country controller

Maria, living in Italy, books a room in a hotel in New York by means of an online EEA travel agency. Maria's personal data, necessary for booking the hotel, are collected by the EEA online travel agency as a controller and sent to the hotel receiving the data as a separate controller. While passing the personal data to the third country hotel, the EEA travel agency carries out a transfer of personal data and Chapter V GDPR applies.



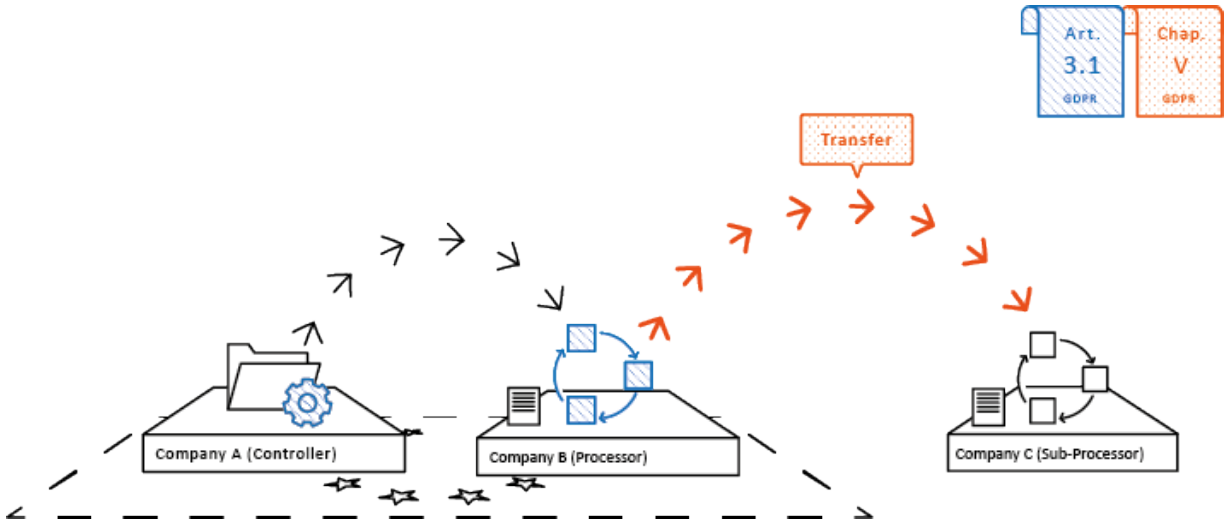
Example 5: Controller in the EU sends data to a processor in a third country

Company X established in Austria, acting as controller, provides personal data of its employees or customers to Company Z in a third country, which processes these data as processor on behalf of Company 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.



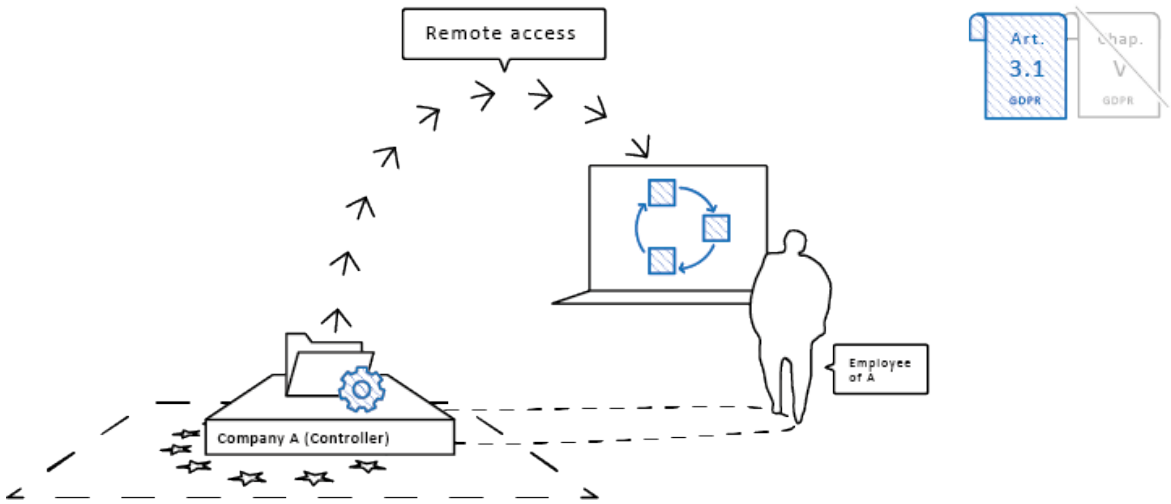
Example 6: Processor in the EU sends data back to its controller in a third country

XYZ Inc., a controller without an EU establishment, sends personal data of its employees/customers, all of them data subjects not located in the EU, 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.



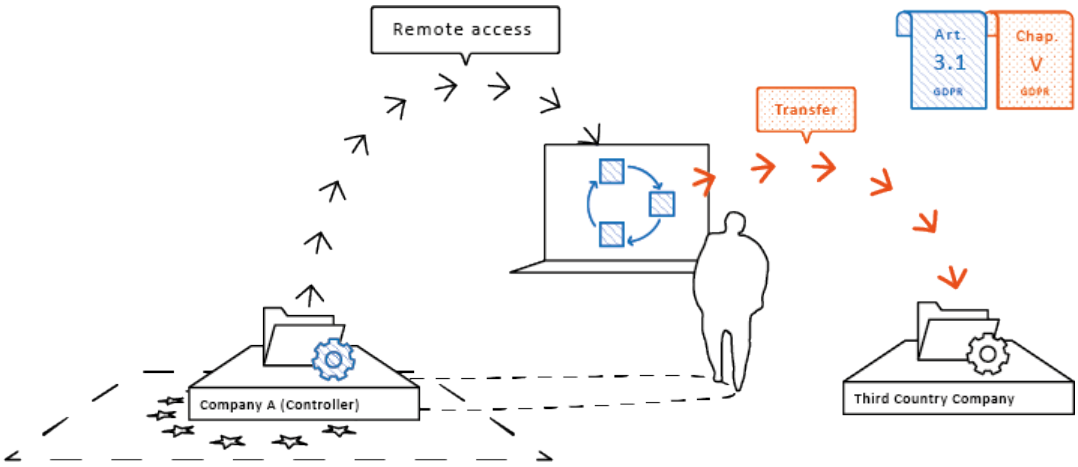
Example 7: Processor in the EU sends data to a sub-processor in a third country

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 in a third country, 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.



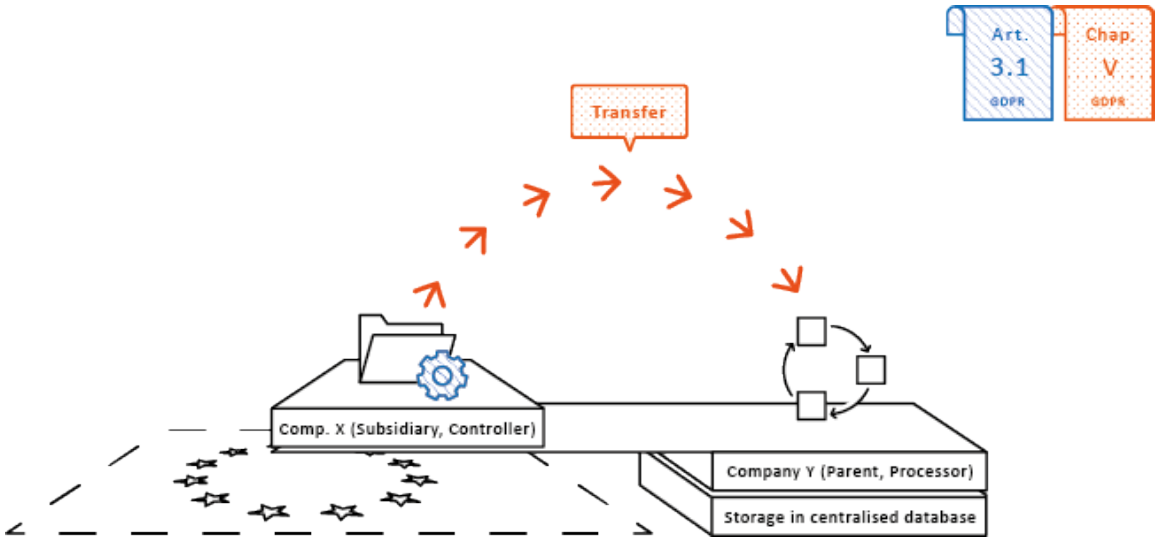
Example 8.1: Employee of a controller in the EU travels to a third country on a business trip

George, employee of A, a company based in Poland, travels to a third country for a meeting bringing his laptop. During his stay abroad, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This bringing of the laptop and remote access of personal data from a third country, does not qualify as a transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (A). Therefore, the transmission 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.



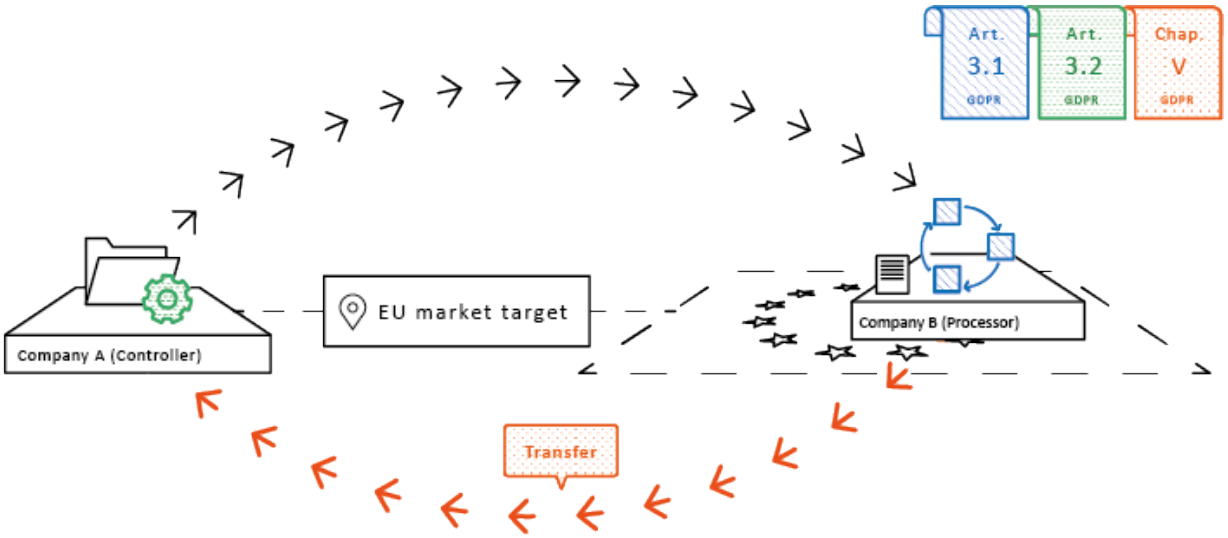
Example 8.2: Employee of a controller in the EU travels to a third country on a business trip

George, employee of A, a company based in Poland, travels to a third country for a meeting bringing his laptop. During his stay abroad, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This bringing of the laptop and remote access of personal data from a third country, does not qualify as a transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (A). Therefore, the transmission 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. It can, however, be noted that in case George, in his capacity as an employee of A, would send or make data available to another controller or processor in the third country, the data flow in question would amount to a transfer under Chapter V; from the exporter (A) in the EU to such importer in the third country.



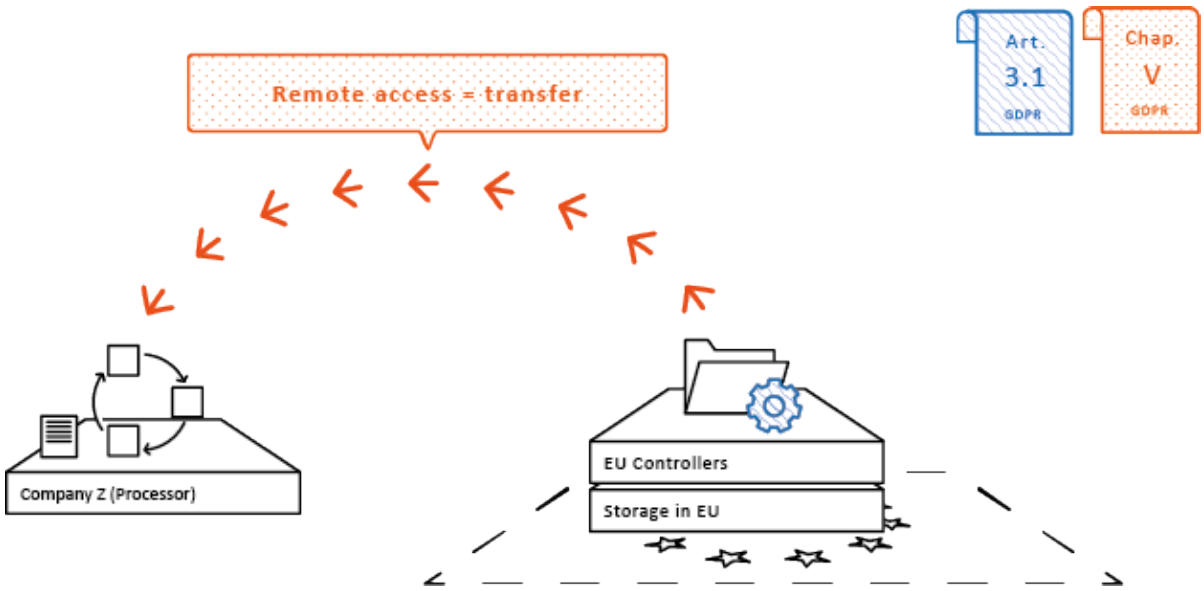
Example 9: A subsidiary (controller) in the EU shares data with its parent company (processor) in a third country

The Irish Company X, which is a subsidiary of the parent Company Y in a third country, discloses personal data of its employees to Company Y to be stored in a centralised HR database by the parent company in the third country. In this case the Irish Company X processes (and discloses) the data in its capacity of employer and hence as a controller, while the parent company is a processor. Company X is subject to the GDPR pursuant to Article 3(1) for this processing and Company Y 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.



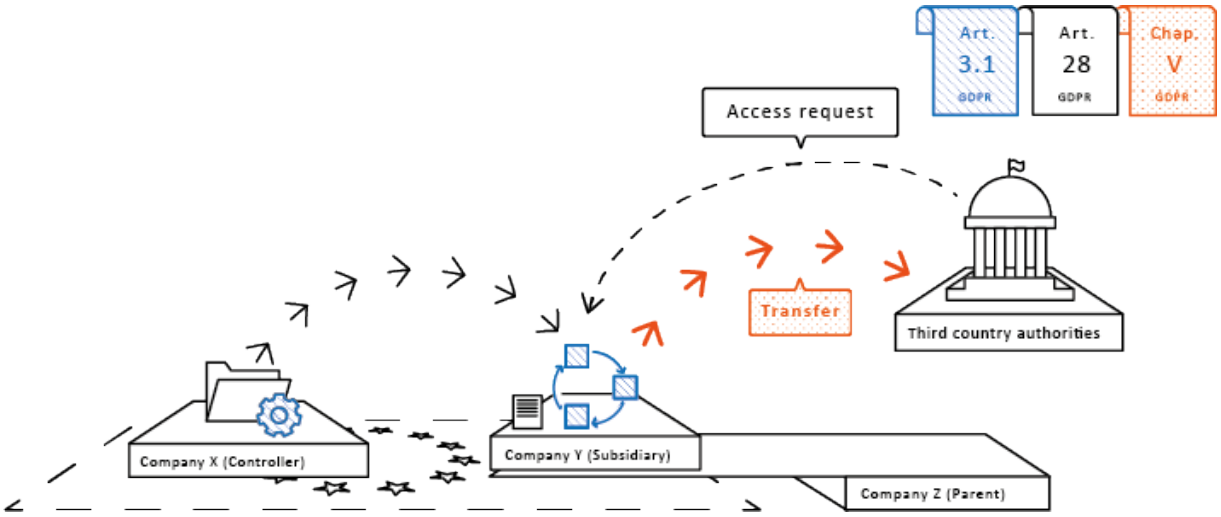
Example 10: Processor in the EU sends data back to its controller in a third country

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.



Example 11: Remote access to data in the EU by a third country processor acting on behalf of EU controllers

A company in a third country (Company Z), with no establishment in the EU, offers services as a processor to companies in the EU. Company Z, acting as processor on behalf of the EU controllers, is remotely accessing, e.g. for support purposes, the data which is stored in the EU. Since Company Z is located in a third country, such remote access results in transfers of data from the EU controllers to their processor (Company Z) in a third country under Chapter V.



Example 12: Controller in the EU uses a processor in the EU subject to third country legislation

The Danish Company X, acting as controller, engages Company Y established in the EU as a processor on its behalf. Company Y is a subsidiary of the third country parent Company Z. Company Y is processing the data of Company X exclusively in the EU and there is no one outside the EU, including the parent Company Z, who has access to the data. Additionally, it follows from the contract between Company X and Company Y that Company Y shall only process the personal data on documented instructions from Company X, unless required to do so by EU or Member State law to which Company Y is subject. Company Y is however subject to third country legislation with extraterritorial effect, which in this case means that Company Y may receive access requests from third country authorities. Since Company Y is not in a third country (but an EU company subject to Article 3(1) GDPR), the disclosure of data from the controller Company X to the processor Company Y does not amount to a transfer and Chapter V of the GDPR does not apply. As mentioned, there is however a possibility that Company Y receives access requests from third country authorities and should Company Y comply with such request, such disclosure of data would be considered a transfer under Chapter V. Where Company Y complies with a request in violation of the controller's instructions and thus Article 28 GDPR, Company Y shall be considered an independent controller of that processing under Article 28(10) GDPR. In this situation, the controller Company X should, before engaging the processor, assess these circumstances in order to ensure that, as required by Article 28 GDPR, it only uses processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing is in line with the GDPR, including Chapter V, as well as to ensure that there is a contract or legal act governing the processing by the processor.