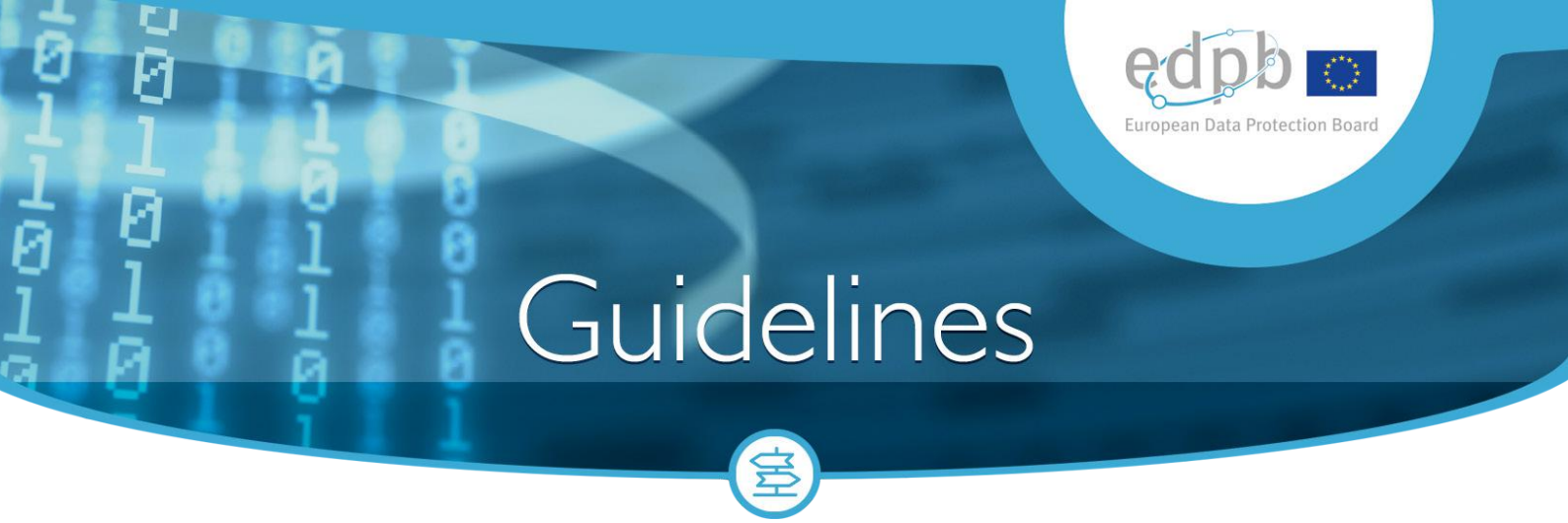


Guidelines 07/2022 on certification as a tool for transfers

Version 2.0

Adopted on 14 February 2023

VERSION HISTORY

Version 1.0	14 June 2022	Adoption of the Guidelines for public consultation
Version 2.0	14 February 2023	Adoption of the Guidelines after public consultation

EXECUTIVE SUMMARY

The GDPR requires in its Article 46 that data exporters shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR diversifies the appropriate safeguards that may be used by data exporters under Article 46 for framing transfers to third countries by introducing, amongst others, certification as a new transfer mechanism (Articles 42 (2) and 46 (2) (f) GDPR).

These guidelines provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification. The document is structured in four sections with an Annex.

Part one of this document ("GENERAL") clarifies that the guidelines supplement the already existing general Guidelines 1/2018 on certification and addresses specific requirements from Chapter V of the GDPR when certification is used as a transfer tool. According to Article 44 of the GDPR, any transfer of personal data to third countries or international organisations, must meet the conditions of the other provisions of the GDPR in addition to complying with Chapter V of the GDPR. Therefore, as a first step, compliance with the general provisions of the GDPR must be ensured and, as a second step, the provisions of Chapter V of the GDPR must be complied with. The actors who are involved and their core roles in this context are described, with a special focus on the role of the data importer who will be granted a certification and of the data exporter who will use it as a tool to frame its transfers (considering that the responsibility for data processing compliance remains with the data exporter). In this context the certification can also include measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Part one of the guidelines also contains information on the process for obtaining a certification to be used as tool for transfers.

The second part of these guidelines (“IMPLEMENTING GUIDANCE ON THE ACCREDITATION REQUIREMENTS”) recalls that the requirements for accreditation of a certification body are to be found in ISO 17065 and by interpreting the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR and its Annex against the background of Chapter V. However, in the context of a transfer, these guidelines further explain some of the accreditation requirements applicable to the certification body.

The third part of these guidelines ("SPECIFIC CERTIFICATION CRITERIA") provides for guidance on the certification criteria already listed in Guidelines 1/2018 and establishes additional specific criteria that should be included in a certification mechanism to be used as a tool for transfers to third countries. These criteria cover the assessment of the third country legislation, the general obligations of exporters and importers, rules on onward transfers, redress and enforcement, process and actions for situations in which national legislation and practices prevents compliance with commitments taken as part of certification and requests for data access by third country authorities.

Part four of these guidelines (“BINDING AND ENFORCEABLE COMMITMENTS TO BE IMPLEMENTED“) provides elements that should be addressed in the binding and enforceable commitments that controllers or processors not subject to the GDPR should take for the purpose of providing appropriate safeguards to data transferred to third countries. These commitments, which may be set out in different instruments including contracts, shall in particular include a warranty that the importer has no reason to believe that the laws and practices in the third country applicable to the processing at stake, including any requirements to disclose personal data or measures authorising access by public authorities, prevent it from fulfilling its commitments under the certification.

The ANNEX of these guidelines contains some examples of supplementary measures in line with those listed in Annex II Recommendations 01/2020 (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data) in the context of the use of a certification as a tool for transfers. Examples are constructed with a view to raise attention to critical situations.

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 "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 GENERAL

1.1 Purpose and scope

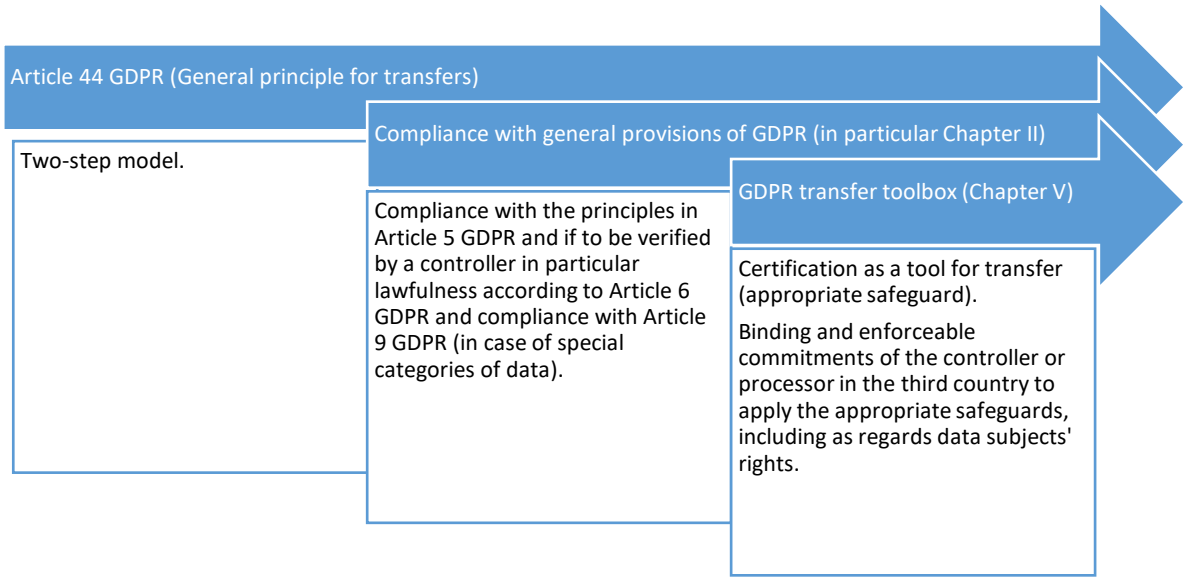
1. This document seeks to provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification. The EDPB has already published general guidance on certification[2] and accreditation[3] under the GDPR. These new guidelines therefore only reflect the specific aspects regarding certification as a tool for transfers. They specify the application of Articles 46 (2) (f) and 42 (2) of the GDPR by providing practical guidance in this respect and introducing new elements to the already published guidelines.

2. The EDPB will evaluate the functioning of these guidelines in light of the experience gained with their application in practice and provide further guidance to clarify the application of the elements listed below including the role of certification agreement with regard to the binding and enforceable commitments referred to in Art. 46 (2) (f) of the GDPR.

1.2 General rules applicable to international transfers

3. According to Article 44 of the GDPR, any transfer of personal data to third countries[4] or international organisations must meet the conditions of the other provisions of the GDPR in addition to complying with Chapter V of the GDPR. Therefore, each transfer must comply inter alia with the data protection principles in Article 5 GDPR, be lawful in accordance with Article 6 GDPR and comply with Article 9 GDPR in case of special categories of data. Hence, a two-step test must be applied. As a first step, compliance with the general provisions of the GDPR must be ensured and as a second step, the provisions of Chapter V of the GDPR must be complied with.

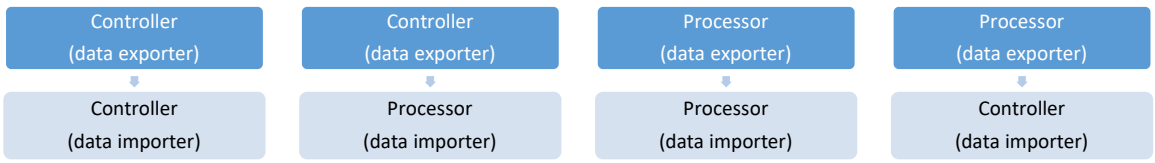
[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.
[3] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).
[4] 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, page 4.



4. The GDPR specifies in its Article 46 that "in the absence of a decision pursuant to Article 45 (3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processors has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available". Pursuant to Article 46 (2) (f) of the GDPR, such appropriate safeguards may be provided for by an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

5. As a result, the data exporter might decide to rely on the certification obtained by a data importer as an element to demonstrate compliance with its obligations e.g. according to Article 24 (3) or Article 28 (5) GDPR. The data importer might decide to apply for certification to demonstrate that appropriate safeguards are in place.

6. Both, the data exporter and the data importer can fulfil different roles (for example as a controller or processor)[5], depending on the processing within Chapter V, which lead to different responsibilities:



7. Aside from the use of certification or any of the other transfer tools or mechanisms referred to in Articles 45 and 46, Article 49 of the GDPR stipulates that in a limited number of specific situations, international data transfers may take place when no other mechanism in Chapter V is complied with[6]. However, as explained in previous guidance issued by the EDPB, the derogations provided by Article

[5] See below: IMPLEMENTING GUIDANCE ON THE CERTIFICATION CRITERIA.
[6] For further information on Article 49 and its interplay with Article 46 in general, please see Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

49 GDPR must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive[7].

1.3 Who are the actors involved and what is their role for certification as a tool for transfers?

8. The **European Data Protection Board (EDPB)** is empowered to approve EEA-wide certification criteria (European Data Protection Seal) and to provide opinions on Supervisory Authorities' draft decisions on certification criteria and accreditation requirements of the certification bodies so as to ensure consistency. It is also competent for collating all certification mechanisms and data protection seals and marks in a register and making them publicly available[8].

9. The **Supervisory Authorities (SAs)** approve the certification criteria when the certification mechanism is not a European Data Protection Seal[9]. They might also accredit the certification body, design the certification criteria and issue certification if established by the national law of their Member State[10].

10. The **National Accreditation Body** may accredit third party certification bodies by using ISO 17065 and the SAs additional accreditation requirements, which should be in line with section 2 of these guidelines. In some Member States, the accreditation can be offered as well by the competent SA as well as being carried out by a national accreditation body or by both.

11. The **Scheme owner** is an organisation which has set up certification criteria and the methodology requirements according to which conformity is to be assessed. The organisation carrying out the assessments could be the same organisation that has developed and owns the scheme, but there could be arrangements where one organisation owns the scheme, and another (or more than one other) performs the assessments as Certification body.

12. Depending on national law, alternatively to SAs, the **Certification body** accredited as said above, can issue the certifications[11]. It might design certification criteria and, thus, be scheme owners (see para 11 above). It has to have an establishment in the EEA in particular in order to allow the effective exercise of corrective powers enshrined in Article 58 (2) (f) GDPR. But the certification body might subcontract activities to local experts or establishments outside the EEA which will perform audit activities on its behalf[12]. Nevertheless, a certification body shall not subcontract the decision regarding the granting or non-granting of a certification.

13. The **Data Importer** is the entity (controller or processor) in the third country receiving data from a data exporter.

14. The **Data Exporter** is the entity (controller or processor) transferring data from the EEA to a data importer. The data exporter must ensure compliance with Chapter V.

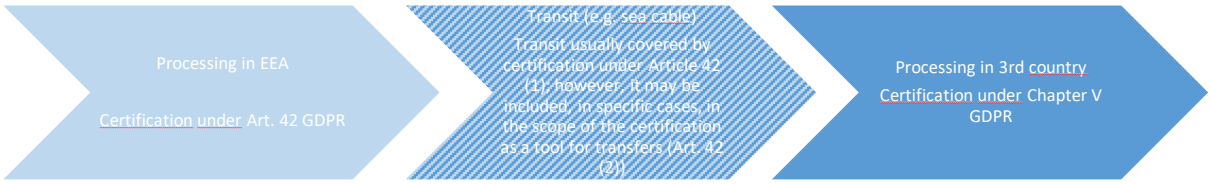
1.4 What are the scope and the object of certification as a tool for transfers?

---

[7] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, page 5.
[8] Article 42(8) GDPR.
[9] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, pt. 2.2.
[10] Articles 42(5) and 43(1) GDPR.
[11] Article 42(5) GDPR.
[12] Certification bodies must assess their local experts in line with ISO 17065 and the additional requirements for accreditation established by the supervisory authority (Article 43 (1) (b) GDPR).

15. A certification mechanism as a transfer tool under Article 42 (2) must aim at ensuring appropriate safeguards for the processing of personal data under the terms of point (f) of Article 46 (2). The certification shall demonstrate the existence of appropriate safeguards provided by controllers or processors outside the EEA or constituting an international organisation receiving data from EEA controllers or processors to counter the specific risks of transferring personal data.

16. In general, the operation of transferring personal data from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR, carried out in a Member State[13] and therefore certifiable under art. 42 (1) GDPR. However, some situations, depending on the context, might include the transit in the scope of the certification as a tool for transfers. Consequently, the object of the certification – which coincides with the Target of Evaluation (ToE) during certification[14] - should generally be the processing of the data received from the EEA by the data importer in the third country and the transit, if under the control of the importer.



17. The object of certification can be a single processing operation or a set of operations. These may comprise governance processes in the sense of organisational measures hence as integral parts of a processing operation[15].

18. The entity applying would, therefore, be the data importer in the third country in relation to its object of certification.

1.5 What should be the role of the exporter in the use of certification as tool for transfers?

19. The transfer by the data exporter as such generally falls directly under the GDPR. This means that the exporter is required to comply with its obligations under the GDPR and in particular to ensure that data is transferred in a secure manner in accordance with Article 32 and Chapter V in order to ensure that the level of protection of natural persons guaranteed by that regulation is not undermined (Article 44 GDPR)[16]. This can, of course, be certified under Article 42 (1).

---

[13] Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, No 83.
[14] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, page 17.
[15] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, page 16 (e.g. complaint handling mechanism).
[16] In this respect, it is 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 sends data to another processor or even to a controller in a third country as instructed by its controller (Article 28(3)(a) GDPR). 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.

20. Furthermore, the data exporter who wants to use a certification as appropriate safeguard according to Article 46 (2) (f) GDPR is notably obliged to verify whether the certification it intends to rely on is effective in light of the characteristics of the intended processing. To that end, the data exporter must check the issued certification in order to verify if the certificate is valid and not expired, if it covers the specific transfer to be carried out and whether the transit of personal data is in the scope of certification, as well as if onward transfers are involved and an adequate documentation is provided on them. Additionally, the exporter has to check that the certification body issuing the certification is accredited by a national accreditation body or a competent supervisory authority. Moreover, the data exporter should refer to using the certification as a tool for transfer in the data processing contract pursuant to Article 28 GDPR in case of transfers from controller to processor or a data-sharing contract with the data importer in case of transfers from controller to controller.

21. Considering that the exporter is responsible for all provisions in Chapter V being applied, it has also to assess whether the certification it intends to rely on as a tool for transfers is effective in the light of the law and practices in force in the third country that are relevant for the transfer at stake. For the purpose of this assessment and as an important element by which to demonstrate compliance with its responsibility, the data exporter may rely on the verification carried out by the certification body of the importer's documented assessment of the third country's laws and practises.

22. In case the importer's assessment has revealed that it and/or the data exporter may need to provide supplementary measures envisaged by the certification to ensure an essentially equivalent level of protection as provided in the EEA, the data exporter must verify the supplementary measures provided by the data importer holding a certification and if it is able to answer the technical and (if any) supplementary measures asked for by the data importer.

23. If those stipulations are not met, the data exporter will have to require from the importer to put in place adapted supplementary measures or establish them by itself.

1.6 What is the process for certification as a tool for transfers?

24. Certification is voluntary, but when sought must be granted via a transparent process based on mandatory rules. The GDPR places considerable trust in private certification mechanisms as a "regulated self-regulation". Accordingly, those mechanisms must ensure that the certificates materially meet the requirements for appropriate safeguards as defined in Article 46 GDPR.

25. Therefore, the certification must be based on the evaluation of certification criteria according to a binding audit methodology. Those criteria will be approved by national SAs or by the EDPB as described in Article 42 (5) GDPR. The criteria for certification shall include requirements for an assessment of the processing performed by the data importer, including onward transfers, and of the third country relevant legal framework, to avoid that the rules and practices of the third country prevent the importer from complying with its obligations under the certification.

26. During the process of certification, the Target of Evaluation shall be checked under certification criteria by a certification body accredited by the national accreditation body or by the competent SA[17].

[17] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), p. 9.

27. According to Article 43 (1) GDPR, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the SA in order to allow it to exercise its powers pursuant to point (h) of Article 58 (2) GDPR where necessary, issue and renew certification.

28. According to Article 43 (5) GDPR, the certification bodies shall provide the competent SAs with the reasons for granting or withdrawing the requested certification. This does not mean that the certification body needs the authorisation of the SA in order to issue certification. The certification body will be monitoring the compliance of its clients with the certification criteria.

29. The SA has the corrective power to withdraw a certification or order to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or order the certification body not to issue certification if the requirements for the certification are no longer met.

30. A European Data Protection Seal for international data transfers may serve as a tool to cover transfers to third countries together with binding and enforceable commitments[18].

31. Nevertheless, certifications to be used as a tool for transfers can also be issued according to national approved certification schemes in EEA States. As such, they are only valid for transfers to third countries from exporters in the EEA Member State where the certification scheme has been approved as there is no mutual recognition of different EEA state certifications. But SAs in different EEA states are free to approve the same certification mechanism for transfers[19].

2 IMPLEMENTING GUIDANCE ON THE ACCREDITATION REQUIREMENTS

32. The requirements for accreditation of a certification body with regard to certifications as a tool for transfers are to be found in ISO 17065 and by interpreting the Guidelines 4/201820 against the background of Chapter V, as explained below.

33. In the opinion of the EDPB, the additional accreditation requirements drafted on the basis of the Guidelines 4/2018 and ISO 17065 adopted according to Article 64 (1) (c) GDPR already cover the specific requirements needed for the accreditation of a certification body with regard to certifications as tool for transfers. However, in a transfer scenario, some requirements need some refinements in term of explanatory notes and interpretation.

34. With regard to the resource requirements (see requirement 6 of the Guidelines 4/2018 - Annex 1) the certification body shall ensure that it has the necessary resources to be able to verify that, as required by the certification criteria, the importer has duly and in a correct way carried out the necessary assessment of the legal situation and practices of the third country/ies where it is established or operates[21]. This assessment should be carried out with respect to the processing activities to be certified

[18] See Article 42 para 5 GDPR and para 35 of EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.
[19] If a SA leads the adoption of the certification criteria X under its national initiative and, afterwards, taking account of the scheme criteria and applicable specific national regulations, other countries want to adopt the same certification criteria, they may adopt the them without triggering an EDPB opinion under article 64 of the GDPR and rely on the opinion given to the first SA, according to Art 64 (3) GDPR (see, in this respect, Reference to Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation), para. 66.
20 Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR and its Annex.
[21] See paragraph 12 above.

as part of the ToE with regard to the appropriate safeguards from Article 46 GDPR, and includes the supplementary measures identified and implemented by the importer, where necessary. This also includes e.g. a significant knowledge of relevant local laws and practices and adequate language skills in relation to the third country/ies.

35. With regard to the process requirements (see requirement 7 of the Guidelines 4/2018 Annex 1) the certification body shall ensure that the process of certification can be backed up by possible on-site audits, is carried out with regard to processing which will take place in the third country/ies, and that the assessment also covers the implementation in practice of existing laws and policies in the third country/ies.

36. With regard to the requirements regarding changes affecting certification (see requirement 7.10 of the Guidelines 4/2018 Annex 1) the certification body shall monitor changes in third country legislation and/or case law that may impact the processing falling within the scope of the ToE.

3 SPECIFIC CERTIFICATION CRITERIA

37. In the context of the consideration of the specific certification criteria, these guidelines are based on the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3. 0), the corresponding Annex 2 on the review and assessment of certification criteria in accordance with Article 42 (5) and the Guidance on Certification criteria assessment Addendum.

38. In the opinion of the EDPB, the certification criteria drafted on the basis of the Guidelines 1/2018 Annex 2 and the Guidance on Certification criteria assessment – Addendum, already cover the majority of the certification criteria which need to be taken into consideration when drafting a certification scheme to be used as tool for transfers. However, there might be a need to further specify some of these existing criteria to tailor them to a specific transfer scenario (see par. 3.1). In addition, there might be a need to formulate additional criteria for the purpose of applying appropriate safeguards, including with regard to the rights of data subjects (see par. 3.2).

3.1 IMPLEMENTING GUIDANCE ON THE CERTIFICATION CRITERIA

39. With regard to the scope of the certification mechanism and target of evaluation (TOE) (see Annex 2, Section 2.a) it should be clearly described in the relevant documentation including with regard to the transfer of personal data to a third country or whether it is intended to cover also their transit.

40. With regard to the scope of the certification mechanism and target of evaluation (TOE) (see Annex 2, Section 2.b) the relevant documentation should describe concretely for which type of entity (ex: controller and/or processor) the certification mechanism is applicable.

41. With regard to the scope of the certification mechanism and target of evaluation (TOE) (see Annex 2, Section 2.f) the criteria should require that the ToE is defined concretely in order to avoid misunderstandings. This should include at least:

42. the processing operation(s), including in case onward transfers are envisaged

    a) the purpose

    b) the type of entity (ex: controller and/or processor)

c) the type of data transferred taking into account whether special categories of personal data as defined in Article 9 GDPR are involved

d) the categories of data subjects

e) the countries where the data processing takes place

43. With regard to Transparency and the Data subjects' rights (see Annex 2, Section 8), the certification criteria should:

a) Require that information on the processing activities should be provided to data subjects, including, where relevant, on the transfer of personal data to a third country or an international organisation (see Articles 12, 13, 14 GDPR)

b) require that data subjects are guaranteed their rights to access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling, essentially equivalent to those provided for by Articles 15 to 19, 21 and 22 GDPR

c) require that an appropriate complaint handling procedure is established by the data importer holding a certification in order to ensure the effective implementation of the data subject rights

d) require assessing whether and to what extent these rights are enforceable for the data subjects in the relevant third country and any additional appropriate measures that may need to be put in place to enforce them, e.g. requiring that the importer will accept to submit itself to the jurisdiction of and cooperate with the supervisory authority competent for the exporter(s) in any procedures aimed at ensuring compliance with these rights and, in particular, that it agrees to respond to enquiries, submit to audits and comply with the measures adopted by aforementioned supervisory authority, including remedial and compensatory measures.

44. With regard to technical and organisational measures guaranteeing protection (Annex 2, Section 10.q), the certification criteria should require the importer to inform the exporter and, if the importer acts as a controller, to notify the SA in the EEA competent for the data exporter(s) of data breaches and to communicate them to the data subjects where the breach is likely to result in a high risk to their rights and freedoms, in line with the requirements of Article 34 GDPR.

3.2 ADDITIONAL SPECIFIC CERTIFICATION CRITERIA

45. In view of the safeguards identified for other transfer instruments under Article 46 of the GDPR (such as binding corporate rules or codes of conduct) and in order to ensure a consistent level of protection, and taking into account the Schrems II ruling of the ECJ, the EDPB considers that certification mechanism to be used as a tool for transfers to third countries, should include also the criteria listed below.

1. Assessment of the third country legislation

a) Do the criteria require the importer to have assessed the rules and practices of the third country where it operates and whether they prevent the importer from complying with its commitments under the certification?

b) Do the criteria require the importer to document the assessment of the rules and practices of the third country where it operates and keep the documentation available to the

certification body and upon request to the SA in the EEA competent for the data exporter and to the data exporter?

c) Do the criteria require the importer to have identified and implemented the organisational and technical measures to provide the appropriate safeguards under Article 46 GDPR taking into account the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data?
d) Do the criteria require the importer to document the organisational and technical measures effectively implemented to provide the appropriate safeguards under Article 46 GDPR and keep the documentation available to the certification body and upon request to the competent data protection authorities and to the data exporter?
e) Do the criteria require the importer to have identified and implemented the organisational and technical measures to ensure the security of the personal data transferred, taking into account the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" if the transit is included in the scope of certification as a tool for transfers?
f) Do the criteria require a warranty to the certification body and the exporter that the importer has no reason to believe that the legislation and practices applicable to it may prevent it from fulfilling its obligations under the certification?

2. General obligations of exporters and importers

a) Do the criteria require to lay down in contractual agreements (e.g. in an existing service contract) between exporters and importers a description of the specific transfer to which the certification applies and that third-party beneficiary rights are recognised to the concerned data subjects?

b) Insofar as the criteria require a specific content for these contractual agreements or instruments and a template is provided, do the criteria require that they also be the subject of the evaluation?

3. Rules on onward transfers

a) Do the criteria require that onward transfers are subject to specific safeguards in line with Chapter V GDPR requirements so as to ensure that the level of protection ensured in the EEA will not be undermined and do the criteria require that appropriate documentation is kept available to the certification body and the SA in the EEA competent for the data exporter(s) and to the data exporter upon request?

4. Redress and Enforcement

a) Do the criteria provide that data subjects can enforce their rights as third-party beneficiaries against the data importer before the EEA court of the data subject's habitual residence, or with an international organisation, including for compensation for damage suffered by the data subject in case of non-compliance by the importer with the relevant Certification scheme?
b) Do the criteria enable adequately assessing that an importer is liable in the EEA for the harm suffered by the data subject in case of non-compliance with the relevant Certification scheme?

c) Do the criteria require that data subjects can lodge a complaint against the importer with a supervisory authority in the EEA, in particular in the EEA State of his or her habitual residence, place of work or competent for the data exporter(s)?
d) Do the criteria require that the importer will cooperate with the supervisory authority in the EEA competent for the data exporter(s) and accept to be audited and to be inspected by it (them)**,** take into account its (their) advice and abide by its (their) decisions?

5. Process and actions for situations in which national legislation prevents compliance with commitments taken as part of certification

a) Do the criteria require a commitment that where the data importer in a third country or an international organisation has reasons to believe that changes in the legislation and practices applicable to it may prevent it from fulfilling its obligations under the certification, it will promptly notify this to the certification body and to the data exporter, so that the latter can evaluate whether to immediately stop the transfers?
b) Do the criteria require a description of the steps to be taken (including notifying the exporter in the EEA and taking appropriate additional measures) if the data importer becomes aware of legislation or practises of a third country that prevents compliance with the obligations under the certification, as well as the measures to be taken in case of requests for information from third country authorities (including the obligation to review and, when necessary, challenge the legality of the request and to minimise any information disclosed)?

6. Dealing with requests for data access by third country authorities

a) Do the criteria require that the data importer will promptly inform the data exporter in case of requests for access by third country authorities and take appropriate additional measures?
b) Do the criteria require that transfers as a result of disproportionate access requests by third country public authorities, in particular requests that require massive and indiscriminate transfers of personal data, should not take place?

7. Additional safeguards concerning the exporter

46. Do the criteria require that, where so envisaged, the data importer ensures, also by way of binding requirements in this respect for the data exporter, that the supplementary measures it has identified are matched by corresponding supplementary measures on the part of the data exporter, taking into account the EDPB Recommendations 01/2020 and the use cases, in order to ensure an effective implementation of the importer's supplementary measures?

4 BINDING AND ENFORCEABLE COMMITMENTS TO BE IMPLEMENTED

47. The GDPR requires in its Article 42 (2) that controllers and processors not subject to the GDPR adhering to a certification mechanism intended for transfers take, additionally, binding and enforceable commitments, via contractual or other legally binding instruments[22], to apply the appropriate safeguards provided by the certification mechanism including with regard to the rights of data subjects.

48. As specified by the GDPR, such commitments may be taken by using a contract, which appears as the most straight forward solution. Other instruments could also be used, provided that the controller/processors adhering to the certification mechanism are able to demonstrate the binding and enforceable nature of such other means.

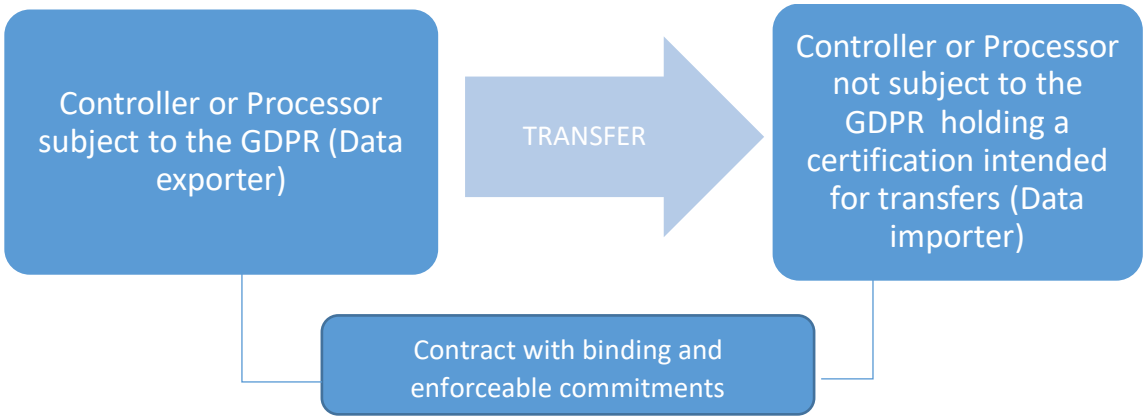
49. In any event, the binding and enforceable nature must be ensured under EU law and the commitments should also be binding and enforceable by data subjects as third-party beneficiaries.

50. A straight forward option would be to include the binding and enforceable commitments in the contract between the data exporter and data importer. In practice, the parties could use an existing contract (e.g. service agreement between the exporter and the data importer, the data processing agreement contract in accordance with Article 28 GDPR between controllers and processors, or a data sharing agreement between separate controllers) in which the binding and enforceable commitments could be included. These commitments should be clearly distinguished from any other clauses. Another option could be to rely on a separate contract for instance by adding to the certification mechanism intended for transfers a model contract that would need to be then signed by controllers/processors in the third country and all of its exporters.

51. There should be flexibility to choose the most appropriate option depending on the specific situation.

52. When the certification mechanism is to be used for transfers and onward transfers by a processor to sub-processors, a reference to the certification mechanism and the instrument providing for binding and enforceable commitments should also be made in the processor agreement signed between the processor and its controller.

Example for binding and enforceable commitments included in the contract between data exporter and data importer:



[22] This legally binding instrument shall not be another Chapter V tool (such as, for example, the SCC), since these binding and enforceable commitments referred to in Article 46(2)(f) have to be designed to ensure that the importer will abide by the certification criteria.

53. In general, the contract or other legally binding instrument must set out that the controller/processor holding a certification acting as an importer commits to comply with the rules specified in the certification intended for transfers when processing the relevant data received from the EEA and warrants it has no reason to believe that the laws and practices in the third country applicable to the processing at stake, including any requirements to disclose personal data or measures authorising access by public authorities, prevent it from fulfilling its commitments under the certification and that it will inform the exporter of any relevant changes in the legislation or practice in this regard.

54. The contract or other instrument shall also provide for mechanisms allowing to enforce such commitments in case of non-compliance with the rules under the certification by the controller/processor acting as an importer, in particular with respect to the rights of data subjects whose data are transferred under the certification.

55. More particularly, the contract or other instrument should address:

- The existence of a right for data subjects whose data are transferred under the certification to enforce as a third-party beneficiaries the commitments taken by the certified data importer under the certification.

- The issue of liability in case of non-compliance with the rules under the certification by a data importer holding a certification outside of the EEA. Data subjects shall have the possibility in case of non-compliance with the rules under the certification by a data importer holding a certification outside the EEA to bring a claim, by invoking their third-party beneficiary right, including for compensation, against that entity before an EEA SA and EEA court of the data subject's habitual residence. The importer holding a certification shall accept the decision of the data subject to do so. Data subjects shall also have the possibility, in case non-compliance by the importer could lead to liability of the data exporter, to bring a claim against the data exporter before the SA or the court of the data exporter's establishment or of the data subject's habitual residence[23]. The data importer and the data exporter should also accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out under Article 80 (1) of the GDPR.

- The existence of a right for the exporter to enforce against the data importer holding a certification the rules under the certification as a third-party beneficiary.

- The existence of an obligation of the data importer holding a certification to notify the exporter and the supervisory authority of the data exporter of any measures taken by the certification body in response to a detected non-compliance with the rules of the certification by the same data importer.

[23] This liability should be without prejudice to the mechanisms to be implemented under the certification with the certification body that can also take action against the certified controllers/processors in accordance with the certification by imposing corrective measures.

ANNEX

A. EXAMPLES OF SUPPLEMENTARY MEASURES TO BE IMPLEMENTED BY THE IMPORTER IN CASE THE TRANSIT IS INCLUDED IN THE SCOPE OF CERTIFICATION

Use case 1: Data storage for backup and other purposes that do not require access to data in the clear

Criteria relating to the encryption standards and the security of the decryption key, in particular criteria relating to the legal situation in the third country, must be established. If the importer can be forced to pass on decryption keys, the additional measure cannot be considered effective[24].

Use case 2: Transfer of pseudonymised Data

In the case of pseudonymised data, criteria shall be established regarding the security of the additional information necessary to attribute the transferred data to an identified or identifiable person, in particular:

- Criteria regarding the legal situation in the third country. If the importer can be forced to access or use additional data in order to attribute the data to an identified or identifiable person, the measure cannot be considered effective[25].

- Criteria relating to the definition of additional information available to third country authorities that might be sufficient to attribute the data to an identified or identifiable person.

Use case 3: Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer

In the case of encrypted data, any criteria for the security of the transit shall be included. If the importer can be forced to pass on cryptographic keys for decryption or authentication or to modify a component used for transit in such a way that its security properties are undermined, the additional measure cannot be considered effective[26].

Use case 4: Protected recipient

In the case of protected recipients, criteria for the limits of the privilege must be defined. The data processing must remain within the limits of the legal privilege. This also applies to processing by (sub) processors and onward transfers, whose recipients must also be privileged[27].

[24] Annex 2, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear, p. 85 ; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf;

[25] See before, paragraph 86-89.

[26] See before, paragraph 90.

[27] See before, paragraph 91.

B. EXAMPLES OF SUPPLEMENTARY MEASURES IN CASE THE TRANSIT IS NOT COVERED BY THE CERTIFICATION AND THE EXPORTER HAS TO ENSURE THEM

Use case 2: Transfer of pseudonymised Data

Criteria shall be provided relating to the additional information available to the third country authorities that might be sufficient to attribute the data to an identified or identifiable person.

Use case 3: Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer

Criteria shall be provided relating to the trustworthiness of the public key certification authority or infrastructure used, the security of the cryptographic keys used for authentication or decryption and the reliability of key management, and the use of properly maintained software without known vulnerabilities.

If the importer can be forced to disclose cryptographic keys suitable for decryption or authentication or to modify a component used for transit in order to undermine its security properties, the measure cannot be considered effective[28].

Use case 4: Protected recipient

In the case of protected recipients, criteria for the limits of the privilege must be defined. The data processing must remain within the limits of the legal privilege. This also applies to processing by (sub)processors and onward transfers, whose recipients must also be privileged[29].

[28] See before Recommendations, paragraph 90.
[29] See before Recommendations, paragraph 91.