

Guidelines



Guidelines 04/2021 on codes of conduct as tools for transfers

Adopted on 07 July 2021

Table of contents

- 1 AIM OF THE GUIDELINES 3
- 2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS? 3
- 3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS? 5
- 4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE? 7
 - 4.1 Code owner 7
 - 4.2 Monitoring body..... 7
 - 4.3 SAs 7
 - 4.4 EDPB 8
 - 4.5 EU Commission..... 8
- 5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS 8
- 6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE? 9
 - 6.1 Binding and enforceable commitments to be implemented 9
 - 6.2 Check-list of elements to be included in a code of conduct intended for transfers..... 11
- Annex 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART..... 13
 - a-The draft code is a “transnational code” and/or a code intended for transfers 13
 - b-The draft code is a “Transnational code” 14

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 AIM OF THE GUIDELINES

1. The aim of these guidelines is to specify the application of Article 40-3 of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries in accordance with Article 46-2-e) of the GDPR. They also aim to provide practical guidance including on the content of such codes of conduct, their adoption process and the actors involved as well as the requirements to be met and guarantees to be provided by a code of conduct for transfers.
2. These guidelines should further act as a clear reference for all SAs, the Board and assist the Commission in evaluating codes in a consistent manner and to streamline the procedures involved in the assessment process. They should also provide greater transparency, ensuring that code owners who intend to seek approval for a code of conduct intended to be used as a tool for transfers (“code(s) intended for transfers” hereafter) are fully aware of the process and understand the formal requirements and the appropriate thresholds required for setting up such a code of conduct.
3. The present guidelines complement the EDPB Guidelines 1/2019 on codes of conduct and Monitoring Bodies under Regulation 2016/679 which establish the general framework for the adoption of codes of conduct. The considerations set out in Guidelines 1/2019 notably regarding the admissibility, submission and criteria for approval are thus also valid in the context of the preparation of codes intended for transfers.

2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS?

4. The GDPR requires in its Article 46 that controllers/processors shall put in place appropriate safeguards for transfers of personal data by to third countries or international organizations.

¹ References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

5. To that end, the GDPR diversifies the appropriate safeguards that may be used by organizations under Article 46 for framing transfers to third countries by introducing amongst others, codes of conduct as a new transfer mechanism (articles 40-3 and 46-2-e). In this respect, as provided by Article 40-3, once approved by the competent SA and having been granted general validity within the Union by the Commission, a code of conduct may also be adhered and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. Such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects as required by Article 40-3.
6. Codes of conduct may be prepared by associations or other bodies representing categories of controllers or processors (code owners) as specified by Article 40-2. As indicated in the EDPB Guidelines 1/2019, a non-exhaustive list of possible code owners would include: trade and representative associations, sectoral organizations, academic organizations and interest groups. According to the same Guidelines, codes intended for transfers could for instance be elaborated by bodies representing a sector (e.g. association/federation from banking and finance, insurance sector) but could also be drawn up for separate sectors which have a common processing activity sharing the same processing characteristics and needs (e.g. HR code drawn up by association/federation of HR professionals, or code on children's data). Such codes would thus allow controllers, processors in third countries, receiving data under the code, to frame these transfers while better addressing the specific processing needs of their sector or common processing activities. As such, they could serve as a more adapted tool compared to other transfer mechanisms that are available under Article 46. Codes of conduct to be used as a tool for transfers will notably allow a given controller or processor in a third country to providing appropriate safeguards for multiple transfers to a third country that are specific to a sector or processing activity. In addition, entities using the codes of conduct do not need to be within the same group to frame their transfers (as is the case for BCRs).
7. It should also be noted that a code intended for transfers adhered by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporter) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controller/processors to adhere to such code themselves. Therefore, a code intended for transfers could frame transfers from controller/processors that do not adhere to that code of conduct to controller/processors in a third country having adhered to that code of conduct, provided that a commitment to comply with the obligations set forth by the code of conduct when processing the transferred data, including with regard to the rights of data subjects, is included in a binding instrument. Groups of companies transferring data from entities subject to the GDPR to those outside of the EEA may also use a code of conduct as a transfer tool where the entities outside the EEA have adhered to that code intended for transfers and have undertaken binding and enforceable commitments related to the transfer. As such, codes intended for transfers may for example be used for framing data flows between organizations not belonging to the same group (e.g. companies in the EEA transferring data to third country organizations operating either in the same or a specific sector) or when a group of companies in a single sector shares data from its entities subject to the GDPR with those outside the EEA.

Example n°1²: Company XYZ is headquartered in Italy and has affiliates in Germany, the Netherlands, Spain and Belgium. For the purpose of managing the IT tools used by the group, Company XYZ uses the services of a cloud service provider based in a third country with no presence in the EU. Data processed as part of the use of IT tools involves transfers of data from Company XYZ and its affiliates to the cloud service provider, for the purpose of storage of data. As the cloud service provider in the third country has adhered to a code of conduct to be used as a tool for transfers relating to cloud services approved under article 40-5, data flows from Company XYZ and its affiliates to the cloud service provider can be framed with the code of conduct to which the cloud service provider has adhered. In this case, the use of a code of conduct by the cloud service provider instead of other transfer tools such as BCRs appears more appropriate to the extent that a code of conduct does not require the controller/processor acting as importers to have a presence in the EEA while a presence in the EEA is required for a group of companies for using BCRs. The code of conduct also presents benefits for addressing multiple transfers of data with a single tool compared to (fully) contractual solutions such as SCCs.

8. A code intended for transfers could also frame transfers from controllers/processors subject to the GDPR and controllers/processors in the third country having adhered to the same code of conduct for transfers, provided in any case as explained above that a commitment to comply with the obligations of the code of conduct including with respect to the rights of data subjects is included in a binding instrument.

Example n°2: An association representing categories of controllers/processors involved in the same type of research activities for the health sector and involving regular transfers of data to third country controller/processors develop a code of conduct which is also intended to be used as a tool for transfers. Relevant controllers/processors in the EEA adhere to this code of conduct which is also being adhered by third country controllers/processors. The transfers of data to third country controller/processors as part of the research activities can be framed with this code of conduct.

9. To the extent that it is most likely that codes intended for transfers would be used by relevant entities for framing transfers from more than one Member State and considering that those CoC should have general validity according to Art. 40-9 GDPR, they would as such qualify as “transnational codes” as defined in the Guidelines 1/2019³.

3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS?

10. As set out above, a code of conduct intended for transfers is one of the tools that can be used by organizations performing particular processing activities - e.g. within a specific sector or a common processing activity which share the same processing characteristics and needs - for providing appropriate safeguards for transfers of personal data to a third country in accordance with Article 46.

²The example is without prejudice to EDPB Recommendations 01/2020 on measures that supplement transfer tools

³ Transnational codes refer to a code which covers processing activities in more than one Member State. See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes

11. Also, the provisions of Article 40-3, which refer to the fact that codes intended for transfers may be adhered by controllers/processors not subject to the GDPR under Article 3, suggest that codes intended for transfers are, in part, or as a whole, more specifically designed for third country controllers/processors. Therefore, according to the EDPB, the object of a code intended for transfers should be to set out also the rules that will need to be complied with by the third country controller/processor (the data importer) to ensure that personal data is adequately protected in line with the requirements of Chapter V GDPR when being processed by such third country controller/processor (i.e. data importer).
12. More specifically in terms of content, for the purpose of providing appropriate safeguards in the meaning of Article 46, the following elements need to be addressed:
 - Essential principles, rights and obligations arising under the GDPR for controllers/processors; and
 - Guarantees that are specific to the context of transfers (such as with respect to the issue of onward transfers, conflict of laws in the third country).
13. In this regard, it is worth noting that a code of conduct may originally be drawn up only for the purpose of specifying the application of the GDPR in accordance with Article 40-2 (“GDPR code”) or also as a code intended for transfers in accordance with Article 40-3. As a consequence, depending on the original scope and content of the code, it may need to be amended in order to cover all of the above mentioned elements if it is to be used as a tool for transfers.

Example n°3: Association ABC gathering organizations operating in the direct marketing sector at EU level has adopted a code of conduct which aims at specifying the application of the transparency principle and associated requirements under the GDPR as part of the processing activities for such sector. The Association wishes to use this code of conduct as a tool for framing transfers outside the EEA. To the extent that the code of conduct is focused on the transparency principle, it would need to be amended in order to cover additionally the appropriate safeguards that are required for international transfers of personal data, all essential principles and main requirements arising under the GDPR (other than transparency) as well as include guarantees that are specific to the context of transfers in order to obtain approval for such code as a code intended for transfers.

14. In any event, in line with the clarifications provided by the EDPB in its guidelines 1/2019, all elements providing for appropriate safeguards as referred above will need to be set out in the code in a manner that facilitates their effective application and specifies how they apply in practice to the specific processing activity or sector⁴.
15. A check-list of the elements to be included in a code intended for transfers so that it can be considered as providing appropriate safeguards is further provided and explained under section 6 of the present guidelines.

⁴ See Guidelines 1/2019, section 6

4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE?

4.1 Code owner

16. The code owner is the entity, association/federation or other body that will prepare a code of conduct intended for transfers or amend an approved “GDPR code” for using it as a tool for transfers and submit it to the competent supervisory authority for approval⁵.

4.2 Monitoring body

17. As for any code of conduct, a monitoring body will need to be identified as part of a code intended for transfers and accredited by the competent SA in line with article 41. More precisely, its role will be to monitor that third country controllers/processors having adhered to such code comply with the rules set out in the code⁶.
18. Considering that codes of conduct intended for transfers are also or more specifically aimed for third country controller/processors, it has to be made sure that monitoring bodies are capable of effectively monitoring the code as specified in the Guidelines 1/2019. Monitoring bodies acting in the framework of codes for transfers could be located either only inside or also outside of the EEA provided that the concerned monitoring body has an establishment in the EEA. In this context, the monitoring body’s establishment in the EEA shall be the one where the headquarters of the monitoring body are, or the place where the final decisions concerning monitoring activities are taken and also requires that an EEA entity shall be able to control the monitoring body’s entities outside the EEA and demonstrate full accountability for all decisions and actions (including its liability for any breaches). In addition, a monitoring body in the EEA may subcontract its activities to an external entity outside the EEA, acting on its behalf, provided that such entity maintains the same competence and expertise as required by the code of conduct as well as by the accreditation requirements, and that the EEA monitoring body is able to ensure effective control over the services provided by the contracting entity and retains the decision making power about monitoring activities.

4.3 SAs

19. In accordance with Article 40-5, the role of the competent Supervisory Authority will be to approve the draft code of conduct intended for transfers or amendment it for using it as a tool for transfers and to accredit the monitoring body identified as part of the code. Where necessary, in the scenario of an amendment to the code of conduct, the SA will accredit the monitoring body, only with respect to additional accreditation requirements relating to codes of conduct for transfers.

⁵ For further details on the requirements relating to the code owner, please refer to the definition of code owner in section 2 and section 5.3 of Guidelines 1/2019

⁶ For further details on the need to set up a monitoring body under a code of conduct, please refer to sections 11 and 12 of Guidelines 1/2019

4.4 EDPB

20. In accordance with Articles 40-7 and 64-1-b, the EDPB will be asked to provide an opinion on the draft decision of a SA aiming to approve a code intended for transfers or amendment to a code of conduct for using it also as a tool for transfers.

4.5 EU Commission

21. As provided by Article 40-9, the Commission may decide by adopting an implementing act that a code intended for transfers and approved by an SA has general validity within the Union. Only those codes having been granted general validity within the Union may be relied upon for framing transfers.

5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS

22. It results from Articles 40-5 and 40-9 that to be adopted, a code intended for transfers shall first be approved by a competent SA in the EEA and then recognized by the Commission as having general validity within the Union by way of implementing act.
23. As mentioned in section 2 above, to the extent that codes intended for transfers are most likely to be used by controllers/processors for framing transfers from more than one Member State, they would as such qualify as “transnational codes” and should follow the procedure for approval for transnational codes, including the need for an Opinion from the EDPB, as specified in section 8 and Annex 4 of the Guidelines 1/2019⁷. In practice different scenarios may arise when an association/federation or other body intends to adopt a code of conduct for transfers:
 - A draft code is designed as a “GDPR code” as well as intended to be used as a tool for transfers by third country controller/processors. Such draft code would first need to be approved by the competent SA according to the procedure for transnational codes, including an Opinion from the Board, and then recognized by the Commission as having general validity within the Union in accordance with Article 40-9. After completion of these steps, controllers/processors in third country may adhere to the code and the code may be used for providing appropriate safeguards for transfers of data to third countries.
 - A code of conduct is initially designed and approved as a “GDPR code”. Such code is further expanded in view of being also used as a tool for transfers by third country controller/processors. The amendment to the code relating to transfers will need to be submitted to the competent SA for approval which will follow the procedure for transnational codes involving an Opinion from the Board. The amended code will then need to be recognized by the Commission as having general validity within the Union in accordance with Article 40-9 after which controllers/in third country may adhere to such code and use it for providing appropriate safeguards for transfers of personal data to third countries.
24. A flow chart set out in the annex to the guidelines details the procedural steps for adopting a code of conduct intended for transfer in consideration of the above possible scenarios.

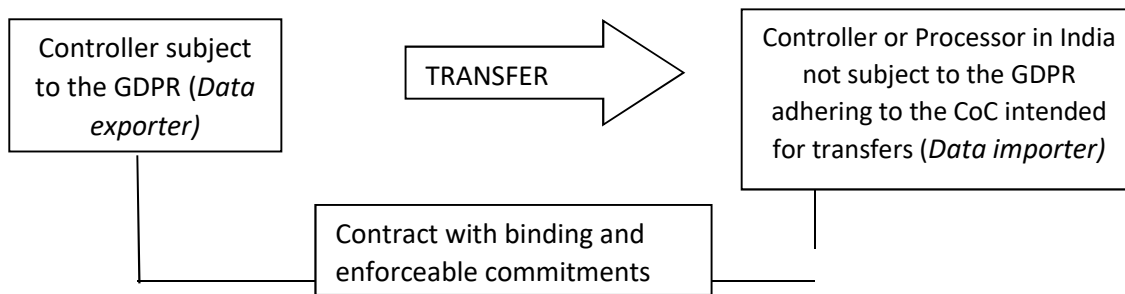
⁷ See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes

6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE?

6.1 Binding and enforceable commitments to be implemented

25. The GDPR requires in its article 40-3 that controllers and processors not subject to the GDPR adhering to a code intended for transfers take binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects.
26. As specified by the GDPR, such commitments may be taken by using a contract, which appears as the most straightforward solution. Other instruments could also be used, provided that these controller/processors adhering to the code are able to demonstrate the binding and enforceable character of such other means.
27. In any event, the instrument needs to have a binding and enforceable nature in accordance with EU law and should also be binding and enforceable by data subjects as third party beneficiaries.
28. A Code of Conduct as a transfer tool can have Code members located in the EEA, as well as Code members located outside the EEA. A distinction between Code members located in the EEA and Code members located outside the EEA is the direct application of the GDPR to the former but not the latter (provided that the latter does not fall under Art 3.2 GDPR).
29. In order to ensure that the Code Member's commitment to adhere to a "specified level of data protection" in a particular sector as set in the code of conduct can be effectively met by both types of Code members, there is a need to ensure that the level of data protection provided for in the GDPR is also committed to by these Code members located outside the EEA. This is a prerequisite for their eligibility to participate in the Code of conduct as a transfer tool. Therefore, the 'binding and enforceable commitments' aim to address this discrepancy between these Code members in the EEA and outside the EEA contractually, and ensures that the 'level of data protection' provided for in the GDPR is ensured also by them.
30. To this end, a contract could, for example, be signed by the controller/processor in the third country (i.e. the data importer) with, the entity transferring data under the code (i.e. data exporter). In practice, the parties could use an existing contract if any (e.g. service agreement between the exporter and the data importer or the contract to be put in place in accordance with article 28 GDPR in case of importer-processors) in which the binding and enforceable commitments could be included. Another option could be to rely on a separate contract for instance by adding to the code 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.
31. Controllers/processors should be able to choose the most appropriate option between the above possibilities depending on their specific situation.
32. When the code of conduct is to be used for transfers and onward transfers by a processor to sub-processors, a reference to the Code of Conduct and the instrument providing for binding and enforceable commitments should also be made in the processor agreement signed between the processor and its controller.

Binding and enforceable commitments with data exporter



33. In general, the contract or other instrument must set out that the controller/processor commits to comply with the rules specified in the code intended for transfers when processing data received under the code. The contract or other instrument shall also provide for mechanisms allowing to enforce such commitments in case of breaches by the controller/processor in particular with respect to the rights of data subjects whose data will be transferred under the code.
34. More particularly, the contract or other instrument should address:
- The existence of a right for data subjects whose data are transferred under the code to enforce the rules under the code as third party beneficiaries;
 - The issue of liability in case of breaches to the rules under the code by code member outside of the EEA. The code shall include a jurisdiction clause noting that data subjects, shall have the possibility in case of violation of rules under the code by a code member outside the EEA to bring a claim, by invoking their third-party beneficiary right, including for compensation, against that entity before a EEA SAs and EEA court of the data subject's habitual residence. The code member outside the EEA shall accept the decision of the data subject to do so. Data subjects shall also have the possibility to bring any claim arising out or from the respect by the importer of the code of conduct against the data exporter before the SA or the court of the data exporter's establishment or of the data subject's habitual residence. This liability should be without prejudice to the mechanisms to be implemented under the code with the monitoring body that can also take action against controllers/processors in accordance with the code by imposing corrective measures. 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 in Article 80(1) of the GDPR.
 - The existence of a right for the exporter to enforce against the code member the rules under the code as a third-party beneficiary
 - The existence of an obligation to notify the exporter and the Supervisory Authority of the data exporter of any detected violation of the code by the code member outside the EEA and of any corrective measures taken by the monitoring body in response to that violation.

6.2 Check-list of elements to be included in a code of conduct intended for transfers

35. In light of safeguards provided by existing transfer tools under article 46 GDPR (such as binding corporate rules), and to ensure consistency in the level of protection, as well as taking into account the CJEU Schrems II ruling⁸, the EDPB is of the view that to be considered as providing appropriate safeguards, the elements to be covered by a code of conduct intended for transfers should include the following:
- A description of transfers to be covered by the code (nature of data transferred, categories of data subjects, countries);
 - A description of the data protection principles to be complied with under the code (transparency, fairness and lawfulness, purpose limitation, data minimization and accuracy, limited storage of data, processing of sensitive data, security, for processors compliance with instructions from the controller), including rules on using processors or sub-processors and rules on onward transfers;
 - Accountability measures to be taken under the code;
 - The setting up of an appropriate governance through DPOs or other privacy staff in charge of compliance with data protection obligations resulting from the code;
 - The existence of a suitable training program on the obligations arising from the code;
 - The existence of a data protection audit (by either internal or external auditors) or other internal mechanism for monitoring compliance with the code, independently from the oversight to be performed by the monitoring body as for any code of conduct; Whereas the aim of the data protection audit program is to ensure and demonstrate compliance with the code, the aim of the audits performed by the monitoring body is to assess whether the applicant is eligible to participate to the code, continues to be eligible once it is a member, and whether sanctions are necessary in case of infringements;
 - Transparency measures, including easy access, regarding the use of the code in particular with respect to third party beneficiary rights;
 - The provision of data subject rights of information, 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 as those provided for by Art. 12, 13, 14, 15, 16, 17, 18, 19, 21, and 22 GDPR;
 - The creation of third-party beneficiary rights for data subjects to enforce the rules of the code as third-party beneficiaries (as well as the possibility to lodge a complaint before the competent SA and before EEA Courts;
 - The existence of an appropriate complaint handling process maintained by the monitoring body which if deemed appropriate may be complemented with an internal procedure to the code member for managing complaints;
 - A warranty that at the time of adhering to the code, the third country controller/processor has no reasons to believe that the laws applicable to the processing of personal data in the third country of transfer, prevent it from fulfilling its obligations under the code and to implement

⁸ Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems;

where necessary together with the exporter supplementary measures⁹ to ensure the required level of protection under EEA law. In addition, a description of the steps to be taken (including notification to the exporter in the EEA, implementation of appropriate supplementary measures) in case after having adhered to the code the third country controller/processor becomes aware of any legislation of the third country preventing compliance by the code member with commitments taken as part of the code and measures to be taken in case of third country government access requests;

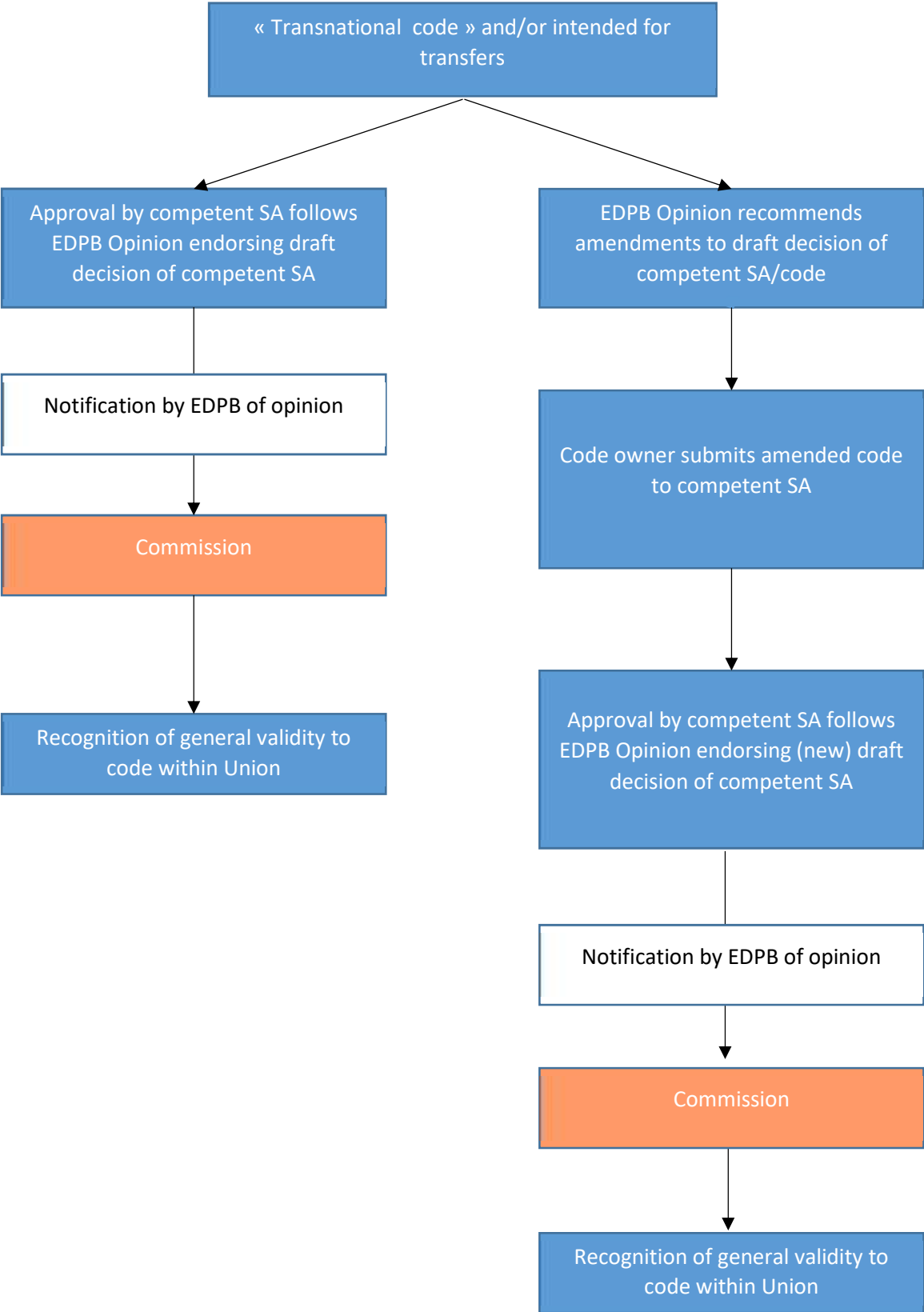
- The mechanisms for dealing with changes to the code;
- The consequences of withdrawal of a member from the code;
- A commitment for the code member and monitoring body to cooperate with EEA SAs;
- A commitment for the code member to accept to be subject to the jurisdiction of EEA SAs in any procedure aimed at ensuring compliance with the code of conduct and EEA Courts;
- The criteria of selection of the monitoring body for a code intended for transfers i.e. to demonstrate that the monitoring body has the requisite level of expertise to carry out its role in an effective manner for such a code intended for transfers

36. In any event, it should be noted that these elements constitute minimum guarantees which may need to be complemented with additional commitments and measures depending on the transfer at stake under the code of conduct.
37. The EDPB will provide further guidance to clarify the application of the above listed elements.

⁹ The European Data Protection Board has published a Recommendation on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data which can assist in the assessment relating to the third country and for identifying appropriate supplementary measures.

ANNEX 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART

a-The draft code is a “transnational code” and/or a code intended for transfers



b-The draft code is a “Transnational code”

