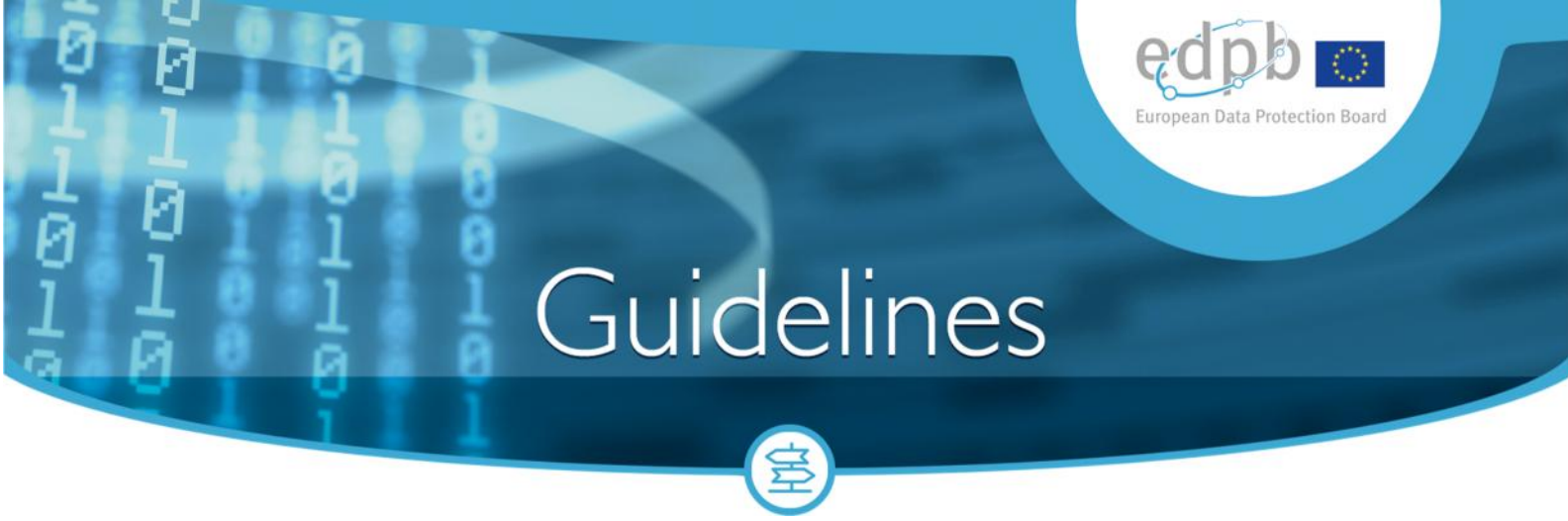

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

Version 2.0

4 June 2019

Adopted

Version history

Version 2.0	4 June 2019	Adoption of the Guidelines after public consultation
Version 1.0	12 February 2019	Adoption of the Guidelines for publication consultation

Table of contents

The European Data Protection Board

Having regard to Article 70(1)(n) and Articles 40 and 41 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,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING OPINION:

1 INTRODUCTION

1. Regulation 2016/679[1] ("the GDPR") came into effect on 25 May 2018. One of the main objectives of the GDPR is to provide a consistent level of data protection throughout the European Union and to prevent divergences hampering the free movement of personal data within the internal market.[2] The GDPR also introduces the principle of accountability, which places the onus on data controllers to be responsible for, and be able to demonstrate compliance with the Regulation.[3] The provisions under Articles 40 and 41 of the GDPR in respect of codes of conduct ("codes") represent a practical, potentially cost effective and meaningful method to achieve greater levels of consistency of protection for data protection rights. Codes can act as a mechanism to demonstrate compliance with the GDPR.[4] Notably, they can help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law.[5] They also provide an opportunity for particular sectors to reflect upon common data processing activities and to agree to bespoke and practical data protection rules, which will meet the needs of the sector as well as the requirements of the GDPR.[6]

[1] The General Data Protection Regulation (EU) 2016/679 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.
[2] See Recital 13 of the GDPR.
[3] See Article 5(2) of the GDPR.
[4] See for example Articles 24(3) and 28(5) and 32(3). A code of conduct may also be used by data processors to demonstrate sufficient guarantees that their processing is compliant with the GDPR (See Article 28(5)).
[5] See Recitals 77, 81, 98, 99, 148, 168 and Articles 24, 28, 35, 40, 41, 46, 57, 64, 70 of the GDPR. This is particularly the case where a code relates to processing activities in several Member States.
[6] Codes do not necessarily need to be confined or limited to a specific sector. For example, a code could apply to separate sectors who have a common processing activity which share the same processing characteristics and needs. Where a code is cross-sectoral in its application, more than one monitoring body may be appointed under that code. However, where this is the case the code should make it absolutely clear as to the scope of that monitoring body's functions, in other words by specifying the sectors in respect of which each monitoring body will perform its functions under Article 41 and the oversight mechanisms available to each monitoring body. In this regard, the relevant sections of these guidelines which set out the responsibilities, obligations and

2. Member States, Supervisory Authorities, the European Data Protection Board ("the Board") and the European Commission ("the Commission") are obliged to encourage the drawing up of codes to contribute to the proper application of the Regulation.[7] These guidelines will support and facilitate "code owners" in drafting, amending or extending codes.

1.1 Scope of these guidelines

3. The aim of these guidelines is to provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR. They are intended to help clarify the procedures and the rules involved in the submission, approval and publication of codes at both a National and European level. They intend to set out the minimum criteria required by a Competent Supervisory Authority ("CompSA") before accepting to carry out an in depth review and evaluation of a code.[8] Further, they intend to set out the factors relating to the content to be taken into account when evaluating whether a particular code provides and contributes to the proper and effective application[9] of the GDPR. Finally, they intend to set out the requirements for the effective monitoring of compliance with a code.[10]

4. These guidelines should also act as a clear framework for all CompSAs, the Board and the Commission to evaluate codes in a consistent manner and to streamline the procedures involved in the assessment process. This framework should also provide greater transparency, ensuring that code owners who intend to seek approval for a code are fully conversant with the process and understand the formal requirements and the appropriate thresholds required for approval.

5. Guidance on codes of conduct as a tool for transfers of data as per Article 40(3) of the GDPR will be considered in separate guidelines to be issued by the EDPB.

6. All codes previously approved[11] will need to be reviewed and re-evaluated in line with the requirements of the GDPR and then resubmitted for approval as per the requirements of Articles 40 and 41 and as per the procedures outlined in this document.

2 DEFINITIONS

'Accreditation' refers to the ascertainment that the proposed monitoring body meets the requirements set out in Article 41 of the GDPR to carry out the monitoring of compliance with a code of conduct. This check is undertaken by the supervisory authority where the code is

accreditation requirements in relation to monitoring bodies apply individually to each such monitoring body appointed under the code.

[7] Article 40(1) of the GDPR.

[8] See Article 40(5), Article 55(1) and Recital 122 of the GDPR.

[9] See Article 40(1) and Recital 98 of the GDPR.

[10] See for example Article 41(2) and 41(3) of the GDPR.

[11] By either National Data Supervisory authorities or the Article 29 Working Party prior to the GDPR and these guidelines.

submitted for approval (Article 41(1)). The accreditation of a monitoring body applies only for a specific code.[12]

'*Code Owners'* refers to associations or other bodies who draw up and submit their code[13] and they will have an appropriate legal status as required by the code and in line with national law.

'*CompSA*' refers to the Supervisory Authority which is competent as per Article 55 of the GDPR.

'*Monitoring body'* refers to a body/committee or a number of bodies/committees (internal or external to the code owners[14]) who carry out a monitoring function to ascertain and assure that the code is complied with as per Article 41.

'Concerned SAs' shall have the same meaning as per Article 4(22) of the GDPR

'National code' refers to a code which covers processing activities contained in one Member State.

'Transnational code' refers to a code which covers processing activities in more than one Member State.

3 WHAT ARE CODES ?

7. GDPR codes are voluntary accountability tools which set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical set of behaviours of a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR compliant data processing activities which give operational meaning to the principles of data protection set out in European and National law.

8. Trade associations or bodies representing a sector can create codes to help their sector comply with the GDPR in an efficient and potentially cost effective way. As provided by the non-exhaustive list contained in Article 40(2) of the GDPR, codes of conduct may notably cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data; the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

[12] However, a monitoring body may be accredited for more than one code provided it satisfies the requirements for accreditation.

[13] As per Recital 98 of the GDPR.

[14] See also Paragraphs 64– 67 below.

9. The GDPR in repealing the Data Protection Directive (95/46/EC) provides more specific and detailed provisions around codes, the requirements which need to be met and the procedures involved in attaining approval, as well as their registration, publication and promotion once approved. Those provisions, in conjunction with these guidelines, will help encourage code owners to have a direct input into the establishment of data protection standards and rules for their processing sectors.

10. It is important to note that codes are one of a number of voluntary tools that can be used from a suite of data protection accountability tools which the GDPR offers, such as Data Protection Impact Assessments (DPIAs)[15] and Certification.[16] They are a mechanism which can be used to assist organisations in demonstrating their compliance with the GDPR.[17]

4 WHAT ARE THE BENEFITS OF CODES?

11. Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost effective manner that takes on board the nuances for a particular sector and/or its processing activities. In this regard codes can be drawn up for controllers and processors taking account of the specific characteristics of processing carried out in certain sectors and the specific needs of micro, small and medium enterprises.[18] They have the potential to be an especially important and beneficial tool for both SMEs and micro enterprise businesses[19] by providing a mechanism which allows them to achieve data protection compliance in a more cost effective way.

> For example, micro enterprises involved in similar health research activities could come together via their relevant associations and collectively develop a code in respect of their collection and processing of health data rather than attempting to carry out such comprehensive data protection analysis on their own. Codes will also benefit supervisory authorities by allowing them to gain a better understanding and insight of the data processing activities of a specific profession, industry or other sector.

12. Codes can help controllers and processors to comply with the GDPR by governing areas such as fair and transparent processing, legitimate interests, security and data protection by design and default measures and controller obligations. Codes are accessible to all processing sectors and can

[15] Codes of Conduct and Certification are voluntary accountability tools, whereas a DPIA will be mandatory in certain circumstances. For further information on other accountability tools please see the general guidance webpage of the EDPB (www.edpb.europa.eu).
[16] See Article 42 of the GDPR and note the EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR.
[17] Adherence to a code does not, of itself, guarantee compliance with the GDPR or immunity for controllers/processors from sanctions or liabilities provided under the GDPR.
[18] See Recital 98 of the GDPR in respect of Article 40(1). For example, a code could be appropriately scaled to meet the requirement of micro organisations in addition to small and medium enterprises.
[19] Article 40(1) of the GDPR in particular identifies codes as a solution to address the needs of such enterprises.

be drafted in as narrow or as wide-ranging a manner as is befitting that particular sector[20], provided that the code contributes to the proper and effective application of the GDPR.[21]

> For example, approval could be sought for a set of rules in respect of how a specific charitable sector would ensure its processing arrangements were fair and transparent. Alternatively, the specific charitable sector could decide to draft a code, which incorporates and properly applies a multitude of different provisions under the GDPR to cover all their processing activities, from the lawful basis for the collection of personal data to the notification of personal data breaches.

13. Codes can provide a degree of co-regulation and they could decrease the level of reliance that controllers and processors may sometimes place upon data protection supervisory authorities to provide more granular guidance for their specific processing activities.

14. Codes can provide a degree of autonomy and control for controllers and processors to formulate and agree best practice rules for their given sectors. They can provide an opportunity to consolidate best practice processing operations in specific fields. They can also become a vital resource that businesses can rely upon to address critical issues in their processing procedures and to achieve better data protection compliance.

15. Codes can provide much needed confidence and legal certainty by providing practical solutions to problems identified by particular sectors in relation to common processing activities. They encourage the development of a collective and consistent approach to the data processing needs of a particular sector.

[20] Article 40(2) of the GDPR refers to codes being prepared by representative organisations of 'categories of controllers and processors'. Therefore this could include cross sector codes where practical provided the representativeness criteria is met.

[21] A narrowly focused code must make it sufficiently clear to data subjects (and to the satisfaction of a CompSA) that controllers/processors adhering to the code does not necessarily ensure compliance with all of the legislation. An appropriate safeguard in this instance could be to ensure adequate transparency regarding the limited scope of the code to those signed up to the code and data subjects.

16. Codes can be an effective tool to earn the trust and confidence of data subjects. They can address a variety of issues, many of which may arise from concerns of the general public or even perceived concerns from within the sector itself, and as such constitute a tool for enhancing transparency towards individuals regarding the processing of their personal data.

> For example, in the context of processing health data for research purposes, concerns over the appropriate measures to be adopted in order to promote compliance with the rules applying to the processing of sensitive health information could be allayed by the existence of an approved and detailed code. Such a code could outline in a fair and transparent manner the following:
>
> - the relevant safeguards to be applied regarding the information to be provided to data subjects;
> - relevant safeguards to be applied in respect of the data collected from third parties;
> - communication or dissemination of the data;
> - the criteria to be implemented to ensure respect for the principle of data minimisation;
> - the specific security measures;
> - appropriate retention schedules; and
> - the mechanisms to manage the data as a result of the exercise of data subjects' rights (As per Articles 32 and 89 of the GDPR)

17. Codes may also provide to be a significant and useful mechanism in the area of international transfers. New provisions in the GDPR allow third parties to agree to adhere to approved codes in order to satisfy legal requirements to provide appropriate safeguards in relation to international transfers of personal data to third countries.[22] Additionally, approved codes of this nature may result in the promotion and cultivation of the level of protection which the GDPR provides to the wider international community while also permitting sustainable legally compliant international transfers of personal data. They may also serve as a mechanism which further develops and fosters data subject trust and confidence in the processing of data outside of the European Economic Area.[23]

18. Approved codes have the potential to act as effective accountability tools for both processors and controllers. As outlined in Recital 77 and Article 24(3) of the GDPR, adherence to an approved code of conduct is envisaged, amongst others, as an appropriate method for a data controller or processor to demonstrate compliance with regard to specific parts or principles of the Regulation

[22] See Article 40(2)(j) and Article 40(3) of the GDPR.
[23] The Board will provide separate guidelines in relation to the use of codes as a mechanism to facilitate international transfers.

or the Regulation as a whole.[24] Adherence to an approved code of conduct will also be a factor taken into consideration by supervisory authorities when evaluating specific features of data processing such as the security aspects[25], assessing the impact of processing under a DPIA[26] or when imposing an administrative fine.[27] In case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority.[28]

5 ADMISSIBILITY OF A DRAFT CODE[29]

19. There are a number of conditions to be met before a CompSA would be in a position to undertake to fully assess and review a code for the purposes of Article 40(5) of the GDPR. They aim to facilitate an efficient evaluation of any draft code. The following criteria apply:

5.1 Explanatory statement and supporting documentation

20. Every draft code which is submitted for approval must contain a clear and concise explanatory statement, which provides details as to the purpose of the code, the scope of the code[30] and how it will facilitate the effective application of this Regulation.[31] This will assist in expediting the process and in providing the requisite clarity to accompany a submission. The submission must also include supporting documentation, where relevant, to underpin the draft code and explanatory statement.[32]

5.2 Representative

21. A code must be submitted by an association/consortium of associations or other bodies representing categories of controllers or processors (code owners) in accordance with Article 40(2). A non-exhaustive list of example of possible code owners would include: trade and representative associations, sectoral organisations, academic organisations and interest groups.

22. The code owners must demonstrate to the CompSA that they are an effective representative body and that they are capable of understanding the needs of their members and clearly defining the

[24] See also Article 24(3) and 28(5) of the GDPR.
[25] Article 32(3) of the GDPR.
[26] Article 35(8) of the GDPR.
[27] Article 83(2) (j) of the GDPR. Also note the application of codes in respect of WP 253/17 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 which was adopted by the EDPB.
[28] *Ibid*
[29] This also applies for all codes (national and transnational) as well as amended or extended codes.
[30] The following non-exhaustive categories may apply: identification of members, processing activity, data subjects, types of data, jurisdictions, concerned SAs (Article 4(22) of the GDPR).
[31] This document provides an opportunity for code owners to demonstrate the rationale and basis for approval of their code. It provides a platform for code owners to outline the appropriateness of safeguards proposed and to demonstrate that proposed mechanisms are fit for purpose.
[32] Examples could include a consultation summary, membership information or research that demonstrates a need for the code.

processing activity or sector to which the code is intended to apply. Depending on the definition and parameters of the sector concerned, representativeness can be derived amongst others from the following elements:

- Number or percentage of potential code members from the relevant controllers or processors in that sector;
- Experience of the representative body with regard to the sector and processing activities concerning the code.

5.3 Processing Scope

23. The draft code must have a defined scope that clearly and precisely determines the processing operations (or characteristics of the processing) of personal data covered by it, as well as the categories of controllers or processors it governs. This will include the processing issues that the code seeks to address and provide practical solutions.

5.4 Territorial scope

24. The draft code must specify whether it is a national or transnational code and provide details in relation to territorial scope, identifying all relevant jurisdictions to which it intends to apply. For any transnational codes (as well as amended or extended transnational codes), a list of concerned SAs must be included. Appendix 1 outlines the distinction between national and transnational codes.

5.5 Submission to a CompSA

25. The code owners must ensure that the supervisory authority chosen to review a draft code is competent in accordance with Article 55 of the GDPR.[33] Appendix 2 provides further information which may assist code owners in choosing a CompSA for a transnational code.

5.6 Oversight of mechanisms

26. The draft code must propose mechanisms that allow for the monitoring of compliance with its provisions by stakeholders who undertake to apply it.[34] This applies to both public and non-public sector codes.

5.7 Monitoring body

27. A draft code which involves processing activities of private, non-public authorities or bodies must also identify a monitoring body and contain mechanisms which enable that body to carry out its

[33] Article 55 of the GDPR states that each supervisory authority is competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the Regulation on the territory of its own Member State. Also see Recital 122 of the GDPR.
[34] See Article 40(4) of the GDPR.

functions as per Article 41 of the GDPR.[35] The identified monitoring body or bodies must have the appropriate standing to meet the requirements of being fully accountable in their role.[36] To this end, the monitoring body or bodies have to be accredited by the CompSA according to Article 41(1) of the GDPR.[37]

5.8 Consultation

28. A draft code must contain information as to the extent of consultation carried out. Recital 99 of the GDPR indicates when drafting a code (or amending/extending) a consultation should take place with the relevant stakeholders including data subjects, where feasible. As such, code owners should confirm and demonstrate that an appropriate level of consultation has taken place with the relevant stakeholders when submitting the code for approval. Where relevant, this will include information about other codes of conduct that potential code members may be subject to and reflect how their code complements other codes. This should also outline the level and nature of consultation which took place with their members, other stakeholders and data subjects or associations/bodies representing them.[38] In practice, a consultation is highly recommended with the members forming part of the organisation or body acting as the code owner and also taking into account the processing activity with the clients of such members. Where no consultation has been carried out with regard to relevant and specific stakeholders due to the lack of feasibility, it will be a matter for the code owner to explain this position.

5.9 National legislation

29. Code owners must provide confirmation that the draft code is in compliance with relevant national legislation, in particular, where the code involves a sector which is governed by specific provisions set out in national law or it concerns processing operations that have to be assessed, taking into account specific requirements and relevant legal obligations under national law.

5.10 Language

30. Code owners should comply with the language requirements of the CompSA to whom they will submit their code. In general, a code should be submitted in the language of the CompSA of that Member State.[39] For transnational codes, the code should be submitted in the language of the CompSA and also in English.[40]

5.11 Checklist

[35] A code involving the public sector will still need to contain suitable mechanisms to monitor the code.
[36] As per Article 83(4) (c) of the GDPR infringements in relation to the obligations of a monitoring body shall be subject to an administrative fine.
[37] See section below entitled 'Accreditation Requirements for Monitoring Bodies' on page 24.
[38] For instance, codes owners could outline how they assessed the submissions received following consultation.
[39] Some Member States may have national legislation which requires a draft code to be submitted in their national language, and it is recommended that code owners explore this issue with the relevant CompSA in advance of formally submitting their draft code for approval.
[40] English is the working language of the EDPB as per Section 23 Rules of Procedure of the EDPB.

31. Ultimately, it will be a matter for the chosen CompSA to determine whether the draft code goes to the next stage of evaluation i.e. a CompSA undertakes to carry out a full assessment of the content in line with Articles 40 and 41 of the GDPR and the procedures detailed below. The Checklist outlined in Appendix 3 should be used to reference documentation submitted to a CompSA and to help frame the submission of the draft code.

6 CRITERIA FOR APPROVING CODES

32. Code owners will need to be able to demonstrate how their code will contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors as well as the specific requirements and obligations of the controllers or processors to whom it relates. There are a number of aspects to this overarching requirement. Code owners should be able to demonstrate that their draft code:

- meets a particular need of that sector or processing activity,
- facilitates the application of the GDPR,
- specifies the application of the GPDR,
- provides sufficient safeguards[41], and
- provides effective mechanisms for monitoring compliance with a code.

6.1 Meets a particular need

33. Code owners are required to demonstrate a need for the establishment of a code. As such a code must address data protection issues which arise for a particular sector or processing activity.

> For example, the sector of information systems for the detection of consumer credit risks may identify a need to formulate a code which provides sufficient safeguards and mechanisms to ensure that the data collected are relevant, accurate and are used exclusively for the specific and legitimate purpose of protecting credit. Similarly, the health research sector may identify a need to formulate a code which provides consistency in approach by setting out standards to adequately meet explicit consent and accompanying accountability requirements under the GDPR.

34. Code owners should be able to explain and set out the problems the code seeks to address and substantiate how the solutions the code offers will be effective and beneficial not only for their members but also for data subjects.

6.2 Facilitates the effective application of the GDPR

[41] For example, 'high risk' sectors, such as processing children's or health data would be expected to contain more robust and stringent safeguards, given the sensitivity of the personal data in question.

35. As per recital 98 of the GDPR, a code, in order to attain approval, will require code owners to be able demonstrate that their code facilitates the effective application of the GDPR. In this regard, a code will need to clearly stipulate its sector-specific application of the GDPR and identify and address such specific needs of a sector.[42]

> For example, providing a list of definitions that are specific to the sector as well as an adequate focus on topics that are particularly relevant to the sector are ways to facilitate the effective application of the GDPR. Using sector-specific terminology to detail the implementation of the requirements of the GDPR in the sector may also improve the clear understanding of the rules by the industry and thus facilitate the effective application of the GDPR. A code should fully take into account the likely risks involved with a particular sector processing activity and appropriately calibrate the related obligations of controllers or processors to whom it applies in light of those risks in that specific sector i.e. providing examples of acceptable terms and conditions in relation to the use of personal data in direct marketing. In terms of format, the content of the code should also be presented in a way that facilitates its understanding, practical use and effective application of the GDPR.

6.3 Specifies the application of the GDPR

36. Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. Codes will need to set out realistic and attainable standards for all their members, and they will need to be of a necessary quality and internal consistency to provide sufficient added value.[43] In other words, a draft code will need to be adequately focused on particular data protection areas[44] and issues in the specific sector to which it applies and it will need to provide sufficiently clear and effective solutions to address those areas and issues.[45]

37. A code should not just re-state the GDPR.[46] Instead, it should aim to codify how the GDPR shall apply in a specific, practical and precise manner. The agreed standards and rules will need to be unambiguous, concrete, attainable and enforceable (testable). Setting out distinct rules in the particular field is an acceptable method by which a code can add value. Using terminology that is unique and relevant to the industry and providing concrete case scenarios or specific examples of 'best practice'[47] may help to meet this requirement.[48]

---

[42] See Article 40(1) of the GDPR.
[43] This standard was first applied in WP 13 DG XV D/5004/98 adopted on 10th September 1998.
[44] Such as those listed in Article 40(2) of the GDPR.
[45] This requirement reflects the previous position of the WP 29 as outlined in Working Document on Codes WP 13 DG XV D/5004/98 adopted on 10th September 1998.
[46] Providing restatements of data protection law was a regular feature of unsuccessful draft codes which were submitted for approval to WP 29.
[47] And 'unacceptable practices'.
[48] A code should avoid, where possible, being overly legalistic.

38. Outlining plans to promote the approved code so individuals are informed of its existence and contents may also assist in reaching the standard of "specifying the application of the GDPR". It is vital that codes are able to provide operational meaning to the principles of data protection as articulated in Article 5 of the GDPR. It is also vital that codes properly take into account relevant opinions and positions published or endorsed by the Board to that particular sector or processing activity.[49] For example, codes containing specifications with regard to processing activities, might also facilitate the identification of adequate legal grounds for these processing activities in the Member States to which they intend to apply.

6.4 Provides sufficient safeguards

39. A code should also meet the requirements of Article 40(5). Approval will only be forthcoming when it is determined that a draft code provides sufficient appropriate safeguards.[50] Codes owners will need to appropriately satisfy a CompSA that their code contains suitable and effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals.[51] It will be a matter for the code owners to provide clear evidence showing that their code will meet these requirements.

> For example, in 'high risk' processing activities such as the large scale processing of children's or health data, profiling or systematic monitoring, it would be expected that the code would contain more demanding requirements upon controllers and processors to reflect an adequate level of protection. Additionally, code owners may benefit from carrying out a more extensive consultation as per Recital 99 of the GDPR to underpin a code involving the processing of such high risk areas.

6.5 Provides mechanisms which will allow for effective oversight

40. As per Article 40(4) of the GDPR, a code requires the implementation of suitable mechanisms to ensure that those rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements. A draft code will also need to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code. Mechanisms may include regular audit and reporting requirements, clear and transparent complaint handling and dispute resolution procedures, concrete sanctions and remedies in cases of violations of the code, as well as policies for reporting breaches of its provisions.

[49] They will also need to fully take on board relevant National and European jurisprudence.
[50] See Recital 98 of the GDPR.
[51] Safeguards may also apply to monitoring bodies and their capabilities in carrying out their role in an effective manner.

41. A draft code will be required to have a monitoring body where it involves processing carried out by non-public authorities and bodies. In essence, a code must not only consider the contents of rules applicable to that sector's processing activity, but it must also implement monitoring mechanisms which will ensure the effective application of those rules. A draft code could successfully propose a number of different monitoring mechanisms where there are multiple monitoring bodies to carry out effective oversight. However, all proposed monitoring mechanisms as to how to give effect to adequate monitoring of a code will need to be clear, suitable, attainable, efficient and enforceable (testable). Code owners will need to set out the rationale and demonstrate why their proposals for monitoring are appropriate and operationally feasible.[52]

7 SUBMISSION, ADMISSIBILITY AND APPROVAL[53] (NATIONAL CODE)

7.1 Submission

42. Code owners should formally submit their draft Code in either an electronic or written (printed/hard copy) format to the CompSA.[54] The CompSA will revert to the code owners acknowledging receipt of the submission, and proceed to carry out a review as to whether the draft code meets the admissibility criteria as set out above[55] before proceeding to carry out a full evaluation of its contents.

7.2 Admissibility of a Code

43. If the draft Code is not accepted on the basis of failing to meet the criteria for admissibility[56] the CompSA will respond to the code owners in writing outlining the basis for its decision. The process would come to an end on this basis and a new submission would be required to be made by the code owners.[57]

44. If the draft code meets the criteria set out above, the CompSA should write to the code owners with confirmation that it will proceed to the next stage of the process and assess the draft code's content in accordance with the relevant procedures provided under national law.

7.3 Approval

[52] The Article 29 Working Party document "Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?" WP7 adopted 14 January 1998 is also an informative document providing further insight into assessing the value of a code and the general grounds required for it to be effective. It is recommended that this document is also considered (where relevant) when formulating a code.

[53] Including amending and extending codes previously approved.

[54] Obviously such an authority will be the National SA for the members to whom the code applies. It is also important that code owners clearly stipulate to the CompSA that they are formally submitting a draft Code for approval and that they clearly indicate the jurisdictional scope of the code. Also please note Appendix 1 in relation to the distinction between national and transnational codes.

[55] See also Appendix 3 checklist.

[56] *Ibid*

[57] It is worth noting that refusal at this stage of the approval process will most likely be based on general or procedural preliminary requirements rather than substantive or core issues associated with the provisions of the draft code.

45. Unless a specific timeline is prescribed under national law, the CompSA should draft an opinion within a reasonable period of time and it should keep the draft owners regularly updated on the process and indicative timelines. The opinion should outline the basis for its decision in line with the criteria for approval as outlined above.[58]

46. If the decision made by the CompSA is to refuse approval, then the process will be completed and it will be a matter for the code owners to assess the findings of the opinion and reconsider the draft code on that basis. It would also be necessary for the code owners to formally re-submit an updated draft code at a later stage, if they choose to do so.

47. If the CompSA approves a draft code, it will be necessary for it to register and publish the code (via its website and/or other appropriate methods of communication).[59] Article 40(11) also requires the Board to make publicly available all approved codes.

8 SUBMISSION, ADMISSIBILITY AND APPROVAL[60] (TRANSNATIONAL CODE)

8.1 Submission

48. Code owners should formally submit their draft code in either an electronic or written format to a CompSA which will act as the principal authority for the approval of the code.[61] The CompSA will revert to the code owners acknowledging receipt of the documentation and proceed to carry out a review as to whether the draft code meets the requirements as set out above[62] before proceeding to carry out a full evaluation of its contents. The CompSA will immediately notify all other supervisory authorities of the submission of a code and provide the salient details which will allow for ease of identification and reference. All supervisory authorities should confirm by return whether they are concerned SAs as per Article 4(22) (a) and (b) of the GDPR.[63]

8.2 Admissibility of a Code

49. If the draft code is not accepted on the basis of failing to meet the admissibility criteria set out above, the CompSA will write to the code owners outlining the basis for its decision. The process

[58] By doing so the CompSA can provide helpful feedback to code owners if they choose to review, amend and re-submit a draft code at a future date.
[59] As per Article 40(6) of the GDPR.
[60] Including amending and extending codes previously approved.
[61] This should be read in the context of the procedure outlined below.
[62] See also Appendix 3 checklist.
[63] This is important as it is envisaged that co-reviewers of the draft code would be supervisory authorities which are concerned by the processing of personal data because the controller or processor is established on the territory of the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing".

will come to an end on this basis and a new submission would be required to be made by the code owners.[64] The CompSA will also issue a notification updating all concerned SAs of the position.

50. If the draft code is accepted by the CompSA on the basis of meeting the admissibility criteria, the CompSA should write to the code owners with confirmation that they will proceed to the next stage of the process and assess the draft code's content. This will trigger the following informal cooperation procedure in respect of assessing the code for approval.

8.3 Cooperation

51. The CompSA will issue a notification updating all SAs[65] of the position, identifying concerned SAs and they will make a request seeking, on a voluntary basis, a maximum of two co-reviewers to assist with the substantive assessment of the draft code. The appointment of co-reviewers will be made on a first come basis.[66] The role of co-reviewers will be to assist the CompSA in assessing the draft code. Once the co-reviewers are confirmed, comments from them on the content of the code should be provided within thirty days from their confirmation as co-reviewers. These comments will then be considered by the CompSA when carrying out its assessment for approval. As per Article 40(7) of the GDPR, the CompSA will make the final determination as to whether the draft decision should be submitted to the Board as per Articles 63 and 64 of the GDPR.[67]

52. The CompSA should aim to arrive at a decision within a reasonable period of time, and it should keep the code owners regularly updated on the progress and indicative timelines. It should outline the basis for its decision (to refuse or to approve a code) in line with the general grounds for approval and communicate that decision in a timely manner to the code owners.

8.4 Refusal

53. If the decision made by the CompSA is to refuse referring a draft code to the Board the process will come to an end and it will be a matter for the code owners to analyse the findings of the decision and reconsider revising their draft code. It would also be necessary for the code owners to resubmit the code for an approval at a later stage, if they choose to do so. The CompSA should also notify all concerned SAs of its position and reasons for refusing to approve a code.

8.5 Preparation for submission to the Board

54. If the CompSA aims to approve the draft code, before submission to the EDPB, the CompSA will circulate its draft approval to all concerned SAs. All concerned SAs will have 30 days to respond

[64] It is worth noting that refusal at this stage of the approval process will most likely be based on general or procedural preliminary requirements rather than substantive or core issues associated with the provision of the draft code.
[65] Concerned SAs should be identifiable from the scope of the draft code.
[66] This request will remain open for ten working days. While co-reviewers are being identified, the CompSA will proceed with the assessment. As a rule, the CompSA will consult two co-reviewers whenever 14 Member States or more are concerned by the code. Under this threshold it is possible to have one or two co-reviewers depending on the specific case.
[67] This can only occur where the CompSA aims to approve the draft code. See Article 40(7) and Article 64(1).

and any significant issues could be brought to the relevant EDPB subgroup for discussion. If the concerned SAs do not respond, the code will proceed to the next stage of the process.

8.6 The Board

55. If the decision is to refer the matter to the Board as per Article 40(7) of the GDPR. The CompSA will communicate that decision to all supervisory authorities as per the consistency mechanisms procedure.[68] The CompSA will also refer the matter to the Board in line with its rules of procedure and Article 40(7) of the GDPR.

56. Under Article 64 the Board shall issue an opinion pertaining to matters outlined in Article 40(7) of the GDPR.[69] The Rules of Procedure of the Board together with the provisions of Article 64 will apply to the Board and the CompSA when conducting an assessment and communicating a decision on the approval of transnational codes.

8.7 Approval

57. The opinion of the Board will be communicated to the CompSA as per Article 64(5) of the GDPR and it will be a matter for the CompSA as to whether it will maintain or amend its draft decision as per Article 40(5).[70] An Opinion of the Board may also be submitted to the Commission pursuant to Article 40(8) and the Board, under Article 40(11), will collate all approved transnational codes and make them publicly available.

9 ENGAGEMENT

58. It is important to note that the assessment process should not serve as an opportunity to further consult on the provisions of the submitted code with the CompSA. The CompSA is tasked, under Article 40(5), to provide an opinion on whether the draft code complies with the GDPR.[71] As such, the communication envisaged between the CompSA and the code owners during this stage of the process will be primarily for the purposes of clarification and to assist in carrying out an evaluation under Article 40 and 41. It is anticipated that code owners will liaise, as appropriate, with supervisory authorities in advance of submitting their draft code for approval. In principle, the approval stage of the process should not invite further consultation by the code owners on particular provisions in the draft code nor should it allow for an extended assessment whereby amendments are continually submitted to the CompSA. It is also imperative that code owners are available to provide answers on points of clarification in respect of their draft code and that they are capable of doing so within a reasonable period of time. It is important that the code owners are prepared and organised to address queries in an efficient and able manner. It is recommended that a single or dedicated point of contact is provided to the CompSA. It will be at the discretion of

[68] See Article 64(4) of the GDPR according to which the views of other supervisory authorities concerned should be presented along with the draft CompSA decision.
[69] See task of Board as per Article 70 (1)(x) of the GDPR.
[70] See Article 64(7) and note the procedures invoked if a CompSA disagrees with the Board's opinion as per Article 64(8) of the GDPR.
[71] The CompSA may also advise and, where relevant, make recommendations to code owners in relation to the content and format of its draft code.

the CompSA as to whether it needs further information before making its decision on the draft code and it will also have discretion to determine the manner of any communication between the parties. For the purposes of continuity, the CompSA will also remain as the principal point of contact during the entire approval process for transnational codes.

10 THE ROLE OF THE COMMISSION

59. The Commission may decide by way of an implementing Act that an approved transnational code will have general validity within the Union and shall ensure appropriate publicity if it were to do so.[72]

11 MONITORING OF A CODE

60. In order for a code (national or transnational) to be approved, a monitoring body (or bodies), must be identified as part of the code and accredited by the CompSA as being capable of effectively monitoring the code.[73] The CompSA will submit its draft requirements for accreditation of a monitoring body to the Board pursuant to the consistency mechanism referred to in Article 63 of the GDPR. Once approved by the Board the requirements can then be applied by the CompSA to accredit a monitoring body.

61. The GDPR does not define the term 'accreditation'. However, Article 41(2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements which should be met in order to satisfy the CompSA to accredit a monitoring body. Code owners will need to explain and demonstrate how their proposed monitoring body meets the requirements set out in Article 41(2) to obtain accreditation.

62. The GDPR provides flexibility around the type and structure of a monitoring body to be accredited under Article 41. Code owners may decide to use external or internal monitoring bodies provided that in both cases the relevant body meets the accreditation requirements of Article 41(2) as outlined in the eight requirements listed below.

12 ACCREDITATION REQUIREMENTS FOR MONITORING BODIES

12.1 Independence

63. The code owners will need to demonstrate that the body concerned is appropriately independent in relation to its impartiality of function from the code members and the profession, industry or sector to which the code applies. Independence could be evidenced through a number of areas

[72] See Article 40(9) and Article 40(10). Such a decision would also permit controllers and processors that are not subject to the GPDR to make binding and enforceable commitments regarding a validated code (See Article 40(3)). This would allow data transfers to third countries or international organisations on the basis that appropriate safeguards are in place and rights and effective legal remedies are available for data subjects (See also Article 46(1) and 46(2)(e)).
[73] GDPR Article 41 (1). Also note that Article 41 does not apply to public authorities or bodies.

such as the monitoring body's funding, appointment of members/staff, decision making process and more generally in terms of its organisational structure. These are considered in more detail below.

64. There are two main models of monitoring which could be used by code owners for fulfilling the monitoring body requirements: external and internal monitoring body. There is some flexibility within these two types of monitoring approaches and different versions could be proposed which are appropriate given the context for the code. Examples of internal monitoring bodies could include an *ad hoc* internal committee or a separate, independent department within the code owner. It will be for the code owners to explain the risk management approach with regard to its impartiality and independence.

65. For instance, where an internal monitoring body is proposed, there should be separate staff and management, accountability and function from other areas of the organisation. This may be achieved in a number of ways, for example, the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body. Similar to a data protection officer, the monitoring body should be able to act free from instructions and shall be protected from any sort of sanctions or interference (whether direct or indirect) as a consequence of the fulfilment of its task.

66. Independence could require that an external counsel or other party having participated in the drafting of the code of conduct, would need to demonstrate that there were appropriate safeguards in place to sufficiently mitigate a risk of independence or a conflict of interest. The monitoring body would need to provide evidence as to the appropriateness of the mechanisms which would satisfactorily identify and mitigate such risks.[74] A monitoring body will need to identify risks to its impartiality on an ongoing basis, such as its activities or from its relationships. If a risk to impartiality is identified, the monitoring body should demonstrate how it removes or minimises such risk and uses an appropriate mechanism for safeguarding impartiality.

67. Independence could also be demonstrated by showing full autonomy for the management of the budget and other resources, in particular in cases where the monitoring body is internal. A monitoring body would also need to be able to act independently in its choice and application of sanctions against a controller or processor adhering to the code. In essence, the body - either internal or external - will need to act independently from code owners and members within the scope of the code in performing its tasks and exercising its powers.

12.2 Conflict of interest[75]

68. It will need to be demonstrated that the exercise of the monitoring body's tasks and duties do not result in a conflict of interests. As such, code owners will need to demonstrate that the proposed monitoring body will refrain from any action that is incompatible with its tasks and duties and that

[74] The context for the code will determine the approach to take. For example, a proposal where there is an adequate separation of duties, whereby the monitoring body personnel did not write, pilot or test the code may suffice.

[75] Impartiality of function, i.e. the ability to act autonomously.

safeguards are put in place to ensure that will not engage with an incompatible occupation. Similarly, the monitoring body must remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person, organisation or association. The body should have its own staff which are chosen by them or some other body independent of the code and it should be subject to the exclusive direction of those bodies only. In the case of an internal monitoring body, it shall be protected from any sort of sanctions or interference (whether direct or indirect) by the code owner, other relevant bodies,[76] or members of the code as a consequence of the fulfilment of its tasks.

12.3 Expertise

69. The code owners will need to be able to demonstrate that the monitoring body has the requisite level of expertise to carry out its role in an effective manner. As such, the submission will need to include details as to the knowledge and experience of the body in respect of data protection law as well as of the particular sector or processing activity. For example, being able to point to previous experience of acting in a monitoring capacity for a particular sector may assist in meeting this requirement. Furthermore, an in-depth understanding of data protection issues and expert knowledge of the specific processing activities which are the subject matter of the code will be welcomed. The staff of the proposed monitoring body should also have appropriate operational experience and training for carrying out the monitoring of compliance such as in the field of auditing, monitoring, or quality assurance activities.

12.4 Established procedures and structures

70. A monitoring body will also need to have appropriate governance structures and procedures which allow it to adequately:

- assess for eligibility of controllers and processors to apply the code;
- to monitor compliance with its provisions; and
- to carry out reviews of the code's operation.

71. Comprehensive vetting procedures should be drafted which adequately assess the eligibility of controllers and processors to sign up to and comply with the code. It should also ensure that the provisions of the code are capable of being met by the controllers and processors.

72. Procedures and structures to actively and effectively monitor compliance by members of the code will be required. These could include random or unannounced audits, annual inspections, regular reporting and the use of questionnaires.[77]The monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code etc. Consideration could be given to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code.

[76] Bodies who represent categories of controllers or processors.
[77] This could also help prevent a situation whereby members are monitored repeatedly while others are not.

73. Code owners will also need to demonstrate that the proposed monitoring body have adequate resources and staffing to carry out its tasks in an appropriate manner. Resources should be proportionate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing.

12.5 Transparent complaints handling

74. A monitoring body will need to establish effective procedures and structures which can deal with complaints handling in an impartial and transparent manner. As such, it needs to have a publicly accessible complaints handling process which is sufficiently resourced to manage complaints and to ensure that decisions of the body are made publicly available.

> For example, evidence of a complaints handling procedure could be a described process to receive, evaluate, track, record and resolve complaints. This could be outlined in publicly available guidance for the code so that a complainant can understand and follow the complaints process. Furthermore, the independence of such processes could be assisted by separate operational staff and management functions in the monitoring body.

75. Monitoring bodies should also have effective procedures to ensure compliance with the code by controllers or processors. An example would be to give the monitoring body powers to suspend or exclude a controller or processor from the code when it acts outside the terms of the code (i.e. corrective measures).

76. If a code member breaks the rules of the code, the monitoring body is obliged to take immediate suitable measures. The aim of suitable corrective measures will be to stop the infringement and to avoid future recurrence. Such remedial actions and sanctions could include such measures ranging from training to issuing a warning, report to the Board of the member, a formal notice requiring the implementation of specific actions within a specified deadline, temporary suspension of the member from the code until remedial action is taken to the definitive exclusion of such member from the code. These measures could be publicised by the monitoring body, especially where there are serious infringements of the code.

77. Where required, the monitoring body should be able to inform the code member, the code owner, the CompSA and all concerned SAs about the measures taken and its justification without undue delay.[78] Moreover, in the case where a Lead Supervisory Authority (LSA)[79] for a transnational code member is identifiable, the monitoring body should also appropriately inform the LSA as to its actions.

12.6 Communication with the competent supervisory authority

[78] If the monitoring is carried out by a body outside the association/body that submits the code of conduct, the code owner should also be informed.
[79] Pursuant to Art. 56 of the GDPR.

78. A proposed monitoring body framework needs to allow for the effective communication of any actions carried out by a monitoring body to the CompSA and other supervisory authorities in respect of the code. This could include decisions concerning the actions taken in cases of infringement of the code by a code member, providing periodic reports on the code, or providing review or audit findings of the code.[80]

79. In addition, it will need to ensure that the supervisory authority is not prejudiced or impeded in its role. For example, a code which proposes that its members can unilaterally approve, withdraw or suspend a monitoring body without any notification and agreement with the CompSA would be in contravention of Article 41(5) of the GDPR.

12.7 Review Mechanisms

80. A code will need to set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR. Review mechanisms should also be put in place to adapt to any changes in the application and interpretation of the law or where there are new technological developments which may have an impact upon the data processing carried out by its members or the provisions of the code.

12.8 Legal status

81. The proposed monitoring body (whether internal or external) and related governance structures will need to be formulated in such a manner whereby the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) and is capable of being fined as per Article 83(4)(c) of the GDPR.

13 APPROVED CODES

82. Clearly the nature and content of the code will determine the roles of the relevant stakeholders in terms of ensuring compliance with the code and the GDPR. However, the CompSA will continue to have a role in ensuring the code remains fit for purpose.

83. The CompSA will therefore work closely with the monitoring body in terms of the reporting requirements arising from the code. The monitoring body will act as the lead contact and coordinator in terms of any issues which may arise in relation to the code.

84. The CompSA would also approve any further amendments or extensions to the code and accredit any new monitoring bodies.[81] As per Article 40(5) of the GDPR, any amendment or extension of an existing code will also have to be submitted a CompSA in line with the procedures outlined in this document.

[80] See Article 41(4).

[81] Amendments requiring approval, for example, could include adding a new code rule, but not updating a reference to the name of an organisation, or other minor changes that do not impact on the operation of the code.

14 REVOCATION OF A MONITORING BODY

85. When a monitoring body does not comply with applicable provisions of the GDPR, a CompSA will also have the powers to revoke the accreditation of a monitoring body under Article 41(5).[82] It is important that the code owner sets out in the Code suitable provisions to address a revocation scenario.

86. However, the consequences of revoking the accreditation of the sole monitoring body for a code may result in the suspension, or permanent withdrawal, of that code due to the loss of the required compliance monitoring. This may adversely affect the reputation or business interests of code members, and may result in a reduction of trust of data subjects or other stakeholders.

87. Where circumstances permit, revocation should only take place after the CompSA has given the monitoring body the opportunity to urgently address issues or make improvements as appropriate within an agreed timescale. In cases which involve transnational codes, the CompSA should, before agreeing to setting parameters with the monitoring body to address the issues raised, liaise with concerned SAs on the matter. The decision to revoke a monitoring body should also be communicated to all concerned SAs and the Board (for the purposes of Article 40(11)).

15 PUBLIC SECTOR CODES

88. Article 41(6) of the GDPR provides that the monitoring of approved codes of conduct will not apply to processing carried out by public authorities or bodies.[83] In essence, this provision removes the requirement for an accredited body to monitor a code. This exemption does not in any way dilute the requirement for the implementation of effective mechanisms to monitor a code. This could be achieved by adapting existing audit requirements to include monitoring of the code.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[82] For transnational codes, it is also essential that the CompSA should ensure that all concerned SAs will be aware of taking such an action. Similarly, for such codes, a concerned SA should also inform the CompSA in cases where a data controller (who is supposed to adopt the code) is found to be non-compliant with it, since this finding may raise concerns on the effectiveness of the monitoring body and the code.

[83] The classification of public sector authorities or bodies is a matter for each member state to determine.

APPENDIX 1 - DISTINCTION BETWEEN NATIONAL AND TRANSNATIONAL CODES

A transnational code refers to a code which relates to processing activities in more than one Member State. As such, a transnational code may relate to processing activities carried out by a multiplicity of controllers or processors in several Member States without necessarily amounting to 'cross-border processing' as defined in Article 4(23) of the GDPR.

Therefore, where a code of conduct adopted by a national association in one Member State covers processing activities by its members in several Member States, it will qualify as a transnational code.

Whereas if an association with a code approved at national level is joined by an international member that conducts cross-border processing, that member could only claim the benefit of the approved code for processing activities in the Member State which approved the code.[84] Mechanisms would need to be put in place to ensure that there is adequate transparency as regards the effective territorial scope of the code.

[84] However, using the same example, it would also be open to the code owners to consider extending the scope of the code and to seek approval for a transnational code.

APPENDIX 2 - CHOOSING A COMPSA

Code owners may have a choice regarding the identification of a CompSA for the purposes of seeking approval of their transnational draft code.[85] The GDPR does not set out specific rules for identifying the CompSA who is most appropriate to carry out an assessment of a draft code. Nevertheless, to assist code owners in identifying the most appropriate CompSA, to evaluate their code, some of the factors which could be taken into account may include the following[86]:

- The location of the largest density of the processing activity or sector;
- The location of the largest density of data subjects affected by the processing activity or sector;
- The location of the code owner's headquarters;
- The location of the proposed monitoring body's headquarters; or
- The initiatives developed by a supervisory authority in a specific field[87];

Whilst these factors are not prescriptive criteria, the decision of choosing a CompSA is important and should be prudently considered. [88] The CompSA role includes, *inter alia,* acting as a single point of contact with the code owners during the approval process, managing the application procedure in its cooperation phase, accrediting the monitoring body (if relevant) and acting as the supervisory lead in ensuring that an approved code is being monitored effectively.

[85] See Article 55 in conjunction with Recital 122 of the GDPR.
[86] This list is non-exhaustive and non-hierarchical.
[87] For example, a Supervisory Authority may have published a detailed and significant policy paper which directly relates to the processing activity which is the subject matter of the code.
[88] A submission for approval of a draft code cannot be refused by a CompSA on the basis that none (or only some) of the non-exhaustive list of criteria outlined in Appendix 2 are met. It can only be refused on the basis of not meeting the criteria outlined in the Section entitled 'Admissibility of a Draft Code'.

APPENDIX 3 - CHECKLIST FOR SUBMISSION

Before submitting a draft code to the competent supervisory authority it is important that you ensure the following (where relevant) have been submitted/set out and are appropriately signposted within the documentation:

1. Have you provided an explanatory statement and all relevant supporting documentation? (Paragraph 20)
2. Are you an association or other body representing categories of controllers or processors? (Paragraph 21)
3. Have you provided details in your submission to substantiate that you are an effective representative body that is capable of understanding the needs of your members? (Paragraph 22)
4. Have you clearly defined the processing activity or sector and the processing problems to which the code is intended to address? (Paragraph 23)
5. Have you identified the territorial scope of your code and included a list of all concerned SAs (where relevant)? (Paragraph 24)
6. Have you provided details to justify the identification of the CompSA? (Paragraph 25)
7. Have you included mechanisms that allow for the effective monitoring of compliance of the code? (Paragraph 26)
8. Have you identified a monitoring body and explained how it will fulfil the code monitoring requirements? (Paragraph 27)
9. Have you included information as to the extent of consultation carried out in developing the code? (Paragraph 28)
10. Have you provided confirmation that the draft code is compliant with Member State law(s) (where relevant)? (Paragraph 29)
11. Have you met the language requirements? (Paragraph 30)

Does your submission include sufficient details to demonstrate the proper application of the GDPR? (Paragraphs 32 – 41)

APPENDIX 4 – TRANSNATIONAL CODE FLOW CHART