EDPB Codes of Conduct Guidelines

Public Consultation: Comments submitted by SRIW e.V. and SCOPE Europe bvba/sprl on "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, adopted on 12 February 2019"

Published and Submitted: **April 2nd, 2019**

1 About SRIW e.V. & SCOPE Europe sprl

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: **SRIW**) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self- and co-regulation. SRIW is also a monitoring body for Data Protection Codes of Conduct in Germany since 2011 and so far has successfully implemented and enforced two codes of conduct in the field of data protection. It further serves as a platform for the development, implementation, enforcement and evaluation of various codes of conduct. SRIW has also actively contributed to the work of the Community of Practice for better self- and co-regulation during its mandate.

SCOPE Europe sprl / bvba (**SCOPE Europe**) is a subsidiary of SRIW. Located in Brussels, it aims to continue and compelement the portfolio of SRIW in Europe and strives to become an accredited monitoring body under the European General Data Protection Regulation. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers and is engaged in other GDPR code of conduct initiatives.

Based on the experience of SRIW and SCOPE Europe (**the authors**), the following comments are made.

SCOPE Europe sprl
Rue de la Science 14
1040 BRUSSELS
https://scope-europe.eu
info@scope-europe.eu

Managing Director
Jörn Wittmann

Company Register: 0671.468.741
VAT: BE 0671.468.74

Selbstregulierung Informationswirtschaft e.V.
Albrechtstraße 10 B
10117 Berlin
https://sriw.de
info@sriw.de

Vorstandsvorsitzender
Harald Lemke
Geschäftsführer
Jörn Wittmann

Amtsgericht Berlin Charlottenburg
Registernummer: VR 30983 B

Table of Contents

2 Preliminary Note

On 12 February 2019, the European Data Protection Board (**EDPB**) issued a public consultation on the *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (**Guidelines**).

As the EBPD invites all interested stakeholders to share their views and concerns[1], SCOPE Europe and SRIW are happy to submit comments on the Guidelines especially focussing on practical experiences SCOPE Europe and SRIW made.

3 General Comments

First of all, these Guidelines are highly appreciated. The Guidelines elaborate purpose and necessity within themselves, as they *"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."*

In general, SCOPE Europe and SRIW very welcome the outlined concepts and aspects of the Guidelines and the covered sections. Their purpose and scope are articulated clearly and the given guidance fosters the implementation of Art. 40 and 41 GDPR in the market. The Guidelines concretize major requirements of GDPR for codes of conduct. This concretization will increase the acceptance by society and industry of codes of conduct as a main instrument to further implement GDPR. The guidance provided helps tremendously to understand the requirements to successfully submit a draft code. Furthermore, the authors want to emphasize the positive impression of flexible and innovation-friendly approaches foreseen by these Guidelines.

The authors very much appreciate the high standards the Guidelines impose on the quality of a monitoring, referring to categories as impartiality or concrete mechanisms to monitor compliance. Only by defining a trusted and common baseline of what must be accomplished by the monitoring of a code of conduct, they will become a valuable, effective and valued tool under GDPR.

[1] European Data Protection Board, accessed on March 4, 2019: https://edpb.europa.eu/our-work-tools/public-consultations-art-704_en.

The authors especially **appreciate** that:

- the Guidelines refer to the *Specification of GDPR* as a main criteria in paragraph 37 of these Guidelines for a valuable code of conduct. The criteria of a code of conduct – *"unambiguous, concrete, attainable and enforceable"* – perfectly reflect the core and very essence of what codes of conduct are about.
- referring to the above-metioned flexibility, the Guidelines pick up on the risk-based approach of GDPR, and acknowledge once more that active and effective monitoring of compliance can and must be variable, to meet the challenges of a safe data processing (e.g.: paragraph 72 of the Guidelines).
- the undertaken distinction between external and internal monitoring body provides a practicable flexibility of structuring and arrangement, but at the same time imposes the same level of impartiality on both concepts as a strict requirement to fulfil for an accreditation (see Chapter 4.5.5 of this Consultation).

Clarification is welcomed:

- on certain terminologies, to safeguard a consistent understandings of key terms (see Chapter 4.1 of this Consultation).
- concerning the scope of these Guidelines as a minimum criteria and its relation to GDPR (see Chapter 4.2 of this Consultation).
- regarding the monitoring body draft requirements, as a guidance for national authorities (see Chapter 4.5 of this Consultation).
- at some points, where different possible interpretations of legal requirements could be taken into consideration, to avoid legal uncertainty in the market (e.g. see Chapters 4.1.3 and 4.4 of this Consultation).

4 Specific Comments

In addition to the General Remarks, please find following some more specific comments:

4.1 Remarks regarding terminology

To avoid fragmentation issues of different interpretations of key terms by each competent national authority, it would be helpful to gain more clarity on certain terminologies. This would contribute to the aim of harmonizing the application of data protection law in Europe.

4.1.1 Accreditation

It is very welcomed that the Guidelines specify which supervisory authority is competent to accredit a monitoring body:

> *'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 submitted for approval (Article 41(1)). The accreditation of a monitoring body applies only for a specific code.* [Chapter 2 (Definitions) of the Guidelines; emphasis by authors]

A code of conduct is inevitably connected to an effective and functioning monitoring body. It can only work as a mechanism of co-regulation, if the monitoring of compliance to a code of conduct is ensured. Combining the approval by the supervisory authority of the code of conduct with the accreditation of the monitoring body follows this legit premise.

Nevertheless, there may be other valuable approaches. From the authors' point of view, the law does not require the CompSA of the code of conduct being identical with the CompSA of the monitoring body. While Art. 40 (5) GDPR mentions the competency of the supervisory authority related to the approval of a code of conduct, Art. 41 GDPR stays silent. Therefore the authors' assessment is that Art. 55 GDPR et seq. would apply directly.

Following this approach, the competence would be determined based on the geographical location, where the monitoring body is registered. SCOPE Europe and SRIW fully support the approach, that any impression of substantially different qualities of monitoring bodies must be prohibited, as such an impression may jeopardize the trust in codes of conduct irrevocably. However, the consistency-mechanism provided by GDPR will ensure that the quality of performance of different monitoring bodies sufficiently. Additionally, if the monitoring body intends to monitor a specific code of conduct, approved by a CompSA in a different country, the CompSA for that accreditation should consult the

CompSA for the approval of the code of conduct to safeguard that the respective monitoring body is capable of monitoring the code of conduct concerned.

If the authors' understanding of determining the CompSA for the accreditation of a monitoring body is not endorsed by the EDPB, further questions with a request for clarification and guidance rise:

- How would the determination of the CompSA, according to the introduced method for the accreditation of the monitoring body, work if multiple monitoring bodies, distributed throughout Europe, would monitor one code of conduct? How would the competence of the then single CompSA conduct with the other national DPAs, where the respective monitoring bodies are located? Clarification on those issues are of utmost importance, as uncertainty about the lawful accreditation may question the applicability of any legal benefits of adhering to a code of conduct and lastly vanish the interest of drafting and adhering to a code of conduct.
- Code owners would be required to look for a potential CompSA to approve their draft code, that could at the same time accredit a monitoring body. As a result, many monitoring bodies could accumulate in one specific country and the respecitive CompSA may automatically be facing requests to monitor a number of codes of conduct. At the same time, code owners may wrongfully avoid choosing a CompSA due to a lack of accredited monitoring bodies in this country. This practical issue could also counteract on the requirements of how the CompSA shall be determined.

4.1.2 Amended Code

As it is required to submit amendments of draft codes to already approved codes for admissibility, (see e.g.: Admissibility of a draft code (Footnote 27, Chapter 5)) some further concretization on the understanding of **amended** is needed and would be valued. Currently „amended" could entail substantive changes or any literal change (even spell-check / grammar-check). From a practical perspective the authors would especially welcome guidance on how to deal with amendments of examples within code of conduct, and if the addition or removal of such an example would be considered as an amendment.

There is an unnumerable variety of possible approaches, that in the authors' experience can be practical, e.g.:

(1) The CompSA shall be notified in case of an change to the code of conduct. Then the CompSA assesses whether the amendment requires re-submission and approval. Provided the

CompSA requires a re-submission necessary, it will forward the amendment to the EDPB, where applicable.

(2) Another approach could be to agree with the CompSA, whilst negoitating the approval of the draft code, what kind of changes would be considered as an amendment and shall be notified and submitted for admissibility, as this could also depend on the content of each code of conduct.

4.1.3 Code Owner

The definition of *Code Owner* in its current version creates some follow-up questions which should be concretized to ensure a practical implementation. The current version states:

> *Code Owners' refers to associations or other bodies who draw up and submit their code and they will have an appropriate legal status as required by the code and in line with national law.* [Chapter 2 (Definitions)]

This results into questions what an *appropriate legal status* shall be and for what purpose this legal status is needed to reasonable assess "appropriateness". From the authors' understanding, the necessity of requiring a legal status could only originate from the need of having a proper addressee in the sense of national state law, for e.g. the approval by the CompSA. Therefore, from a practical perspective an *appropriate legal status* should be defined to serve this purpose – ascertaining that the aforementioned formal need can be met. The authors consider it crucial to provide some guidance on this question, to enable target groups to comply with this definition without legal uncertainties.

4.2 Scope of these Guidelines as minimum criteria

As mentioned above, the aim of these Guidelines is appreciated. Providing practical guidance and interpretative assistance is highly necessary to implement codes of conduct in the market and enhance its application in the European Union. One main mechanism to reach that aim is to standardize the way GDPR and its requirements are handled by the supervisory authorities. Standardization is key to implement codes of conduct in a sustainable way in the market.

Additionally, the Guidelines state that they are intended to set out minimum criteria before accepting to carry out a further evaluation of the draft code:

> *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. (...)* [Scope of these guidelines (Chapter 1.1); emphasis by authors]

Describing these Guidelines as minimum criteria can counteract on the aim of standardization, as it, if understood literally, allows multiple, different requirements per Member State and even conflicting standards.

Therefore, it is important to clarify that the different CompSAs are not allowed to require different or even conflicting standards than the one set out in this guidance. Subsequently, this does not mean overfulfilling these requirements cannot be appreciated by each CompSA. But to harmonize the implementation of codes of conduct in the European Union, the different CompSAs need to act according to the same standards.

Furthermore, these Guidelines do not only reflect minimum criteria, but increase requirements laid down by GDPR itself. This raises questions on the relation between the Guidelines and GDPR and which may prevail in case of conflict.

Examples of this higher standards are:

- Submission of a list of concerned SAs when submitting the draft code(Chapter 4.3.1 of this Consultation)
- Confirmation by the code owners of compliance of the draft code with national legislation (Chapter 4.3.2 of this Consultation)
- Information duty of the monitoring body towards the CompSA and all concerned SAs about all measures taken (see Chapter 4.5.2 of this Consultation)
- Agreement requirement by the CompSA regarding the monitoring body in case members of a respective code of conduct can unilaterally approve, withdraw or suspend a monitoring body (see Chapter 4.5.3 of this Consultation)

From a practical point of view the proposed extension of the conditions as provided by GDPR seems critical. Adhering to a code of conduct is voluntary and makes anybody subject to sanctions and remedies not only imposed by supervisory authorities but also a monitoring body, already. Extended obligations by these Guidelines may jeopardize a general interest in adhering to codes of conduct.

4.3 Formal requirements of submitting a code

It is highly appreciated that these Guidelines set out concrete formal requirements for code owners, if they want to submit the draft code, e.g. including an explanatory document and further supporting

documentation. There are nevertheless some requirements mentioned, that, from the authors' perspective, would need some further clarification to avoid fragmentation caused by different implementation of different national authorities.

4.3.1 List of concerned supervisory authorites

The Guidelines state that the code owners of transnational codes must provide a list of concerned SAs when submitting a draft code:

> *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.* [Territorial Scope (Chapter 5.4); emphasis by authors]

At the same time, other paragraphs seem to chose a different approach regarding this requirement:

> *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. 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 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.* [Chapter 8.1 (Submission); emphasis by authors]

The procedure above can be understood in the following way: all supervisory authorities get a notification of a submitted draft code, with salient details, and based on that, the supervisory authorities themselves notify if they are a concerned supervisory authority or not.

This discrepancies in the wording may create inconsistencies in the implementation by the national authority and therefore create uncertainties in the market, especially as the submission of a list of concerned SAs is not foreseen by GDPR.

Therefore, some alignment in these paragraphs would be appreciated, to standardise who identifies the concerned SAs and to clarify if the code owners need to add a list of all concerned SAs. It might be worth evaluating the idea that code owners have to provide a list of concerned SAs if the respective code of conduct is unambiguously applicable only in certain members states (e.g. if the code of conduct covers a service which is only available in one or some European countries). Regarding all other

transnational codes of conduct, the SAs themselves would decide on their role as concerned SA as outlined in the Guidelines.

4.3.2 Compliance with national legislation

By GDPR and these Guidelines, the application of data protection law shall be harmonized to allow for a regulated flow of personal data inside the European Union. This is well recognized by these Guidelines:

> *Notably, they can help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law.* [Introduction (Chapter 1)]

This aim is well appreciated. To not counteract on this main goal of GDPR and codes of conduct as a mechanism to reach this goal, it could be worth re-evaluating the requirement of code owners to demonstrate that their code of conduct is in compliance with applicable national legislation.

> *29. Code owners must provide confirmation that the draft code is in compliance with applicable 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.* [National Legislation (Chapter 5.9); emphasis by authors]

Generally, it would be helpful to get some clarification what *applicable national legislation* means. If thereby the Guidelines refer to national data protection law, the following should be considered:

GDPR provides that, in some cases, national data protection law may determine additional requirements. Whilst a code of conduct can take into account that such a national derogation may exist, this should not be made a general requirement. Especially as such a mechanism will question the benefits of a transnational code of conduct by providing a certainty on GDPR compliance. Further, a code of conduct stays compliant with GDPR even if there are national derogations, and therefore is still approvable. Also, national derogations may be challenged as GDPR compliant themselves and it is nearly impossible to assess compliance with applicable legislation beyond reasonable doubt. Therefore, there seems to be no added value of a *confirmation* of the compliance with national legislation, especially as a possible non-compliance should not hinder an approval as GDPR compliant. Additionally, it seems unsual to let code owners provide an opinion on a lawful conduct, as the national authorities are best suited to verify this compliance. In order to support the main goals of GDPR, harmonization and legal certainty and consistency throughout Europe, it can only be reasonable to let the

national authorities themselves keep the sovereignty on compliance of the code of conduct in question with possible national derogations.

If *applicable national legislation* addresses anything else than national data protection law, it is of utmost importance to clarify. From a practical perspective such a broad understanding should not be applied. Frictions of different fields of law with data protection laws are again too diverse and often highly disputed.

With this in mind, further guidance or concretization about this topic would be much appreciated.

4.3.3 Language requirement

To reach the goal of effective business implementation of codes of conduct, it must be ensured that these Guidelines are accepted by main stakeholders and hereby accepted in the market. This also includes a functioning communication and understanding in the market. Therefore, for transnational codes of conduct, it needs to be clarified which language requirements must be met. The Guidelines address this in Chapter 5.10:

> *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. For transnational codes, the code should be submitted in the language of the CompSA and also in English.* [Language (Chapter 5.10); emphasis by authors]

The acknowledgement of the need of an English version for transnational codes of conduct is highly appreciated and will contribute to the proper implementation of codes of conduct throughout Europe. It is also highly understandable, that for the CompSA, in order to thoroughly examine the code of conduct, a second version in the language of the CompSA can be helpul. Originating from the point that therefore transnational codes of conduct will always exist in minimum two languages, it is crucial to determine in a standardized way which language shall be binding and therefore prevails in case of conflicts. A possible and also practicable solution would be that this will be the English version, as it would also be the one endorsed by the EDPB.

4.4 Procedure of approval

Chapter 8 concretizes the procedure of submission, acceptance and approval of transnational codes. The concretization and disclosure of the procedure is highly appreciated, as it gives transparency, legal certainty and planning security.

While welcoming the chapter 8 as such, some practical perspectives may be beneficial to further improve this section

4.4.1 Role of the Competent Supervisory Authority

Pursuant to Art. 40 (7) GDPR, the procedure of approving a transnational code of conduct is triggered by the supervisory authority which submits the draft code according to Art. 63 GDPR to the EDPB. The EDPB shall provide an opinion on whether the draft code complies with GDPR. Art. 64 (1) p. 2 (b) GDPR completes this procedure by stating:

> *"To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it concerns a matter pursuant to Art. 40 (7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation."*

Therefore Art. 64 GDPR clarifies that the question of substantive compliance of the draft code with GDPR needs to be answered by the EDPB itself, so that the CompSA can take the answer into consideration when approving or denying the code of conduct. Therefore, this does also imply cases where the CompSA is not convinced by the compliance of the code of conduct, as the EDPB always needs to be considered to answer this question. To concretize this article, the Guidelines state:

> *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. 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 before proceeding to carry out a full evaluation of its contents. Footnote 60: See also Appendix 3 checklist. [Procedure of Approval (Chapter 8);* emphasis by authors]

This clarification seems ambiguous and may even contradict the role of the CompSA as stated above to check the admissibility criteria without an evaluation of content. Further, the Appendix 3 checklist includes as a last question:

> *Does your submission include sufficient details to demonstrate the proper application of the GDPR (paragraph 32-41)?*

Paragraph 49 rightfully sets out that non-acceptance of the draft code could only happen if it is failing **the admissibility criteria**, and in this case, without previous communication of the draft code to the EDPB.

> *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 their decision. The process will come to an end on this basis and a new submission would be required to be made by the code owners. The CompSA will also issue a notification updating all concerned SAs of the position.* [Procedure of Approval (Chapter 8); emphasis by authors]

To ensure consistency with the above explained procedures, this provision could be improved by ensuring that the question in Appendix 3 checklist is **not** understood in a substantive way, but in a formal way. This means, to contribute to the consistent harmonization of data protection throughout Europe, the CompSA should only make sure if the code of conduct contains details that **potentially** demonstrate the proper application of GDPR, leaving the examination whether the code of conduct substantively addresses issues of the proper application of GDPR (or other substantive questions) to the EDPB. In this context, it might also be worth to consider changing footnote 62 to prevent any confusion and to safeguard the appropriate involvement of the EDPB as foreseen in Art. 64 (1) p. 2 (b) GDPR.

> *Footnote 62: 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.* [Procedure of Approval (Chapter 8); emphasis by authors]

4.4.2 Interdependence of code of conduct and monitoring bodies

In the context of the procedure of approval the authors would like to introduce the concept of assessing a code of conduct detached from its monitoring body. In particular, it could be helpful to code owners, at least in some cases, to get into the approval process and focus on substantive matters while the concrete aspects of the monitoring body can be assessed separately. On a pragmatic level, the adoption of codes of conduct might be fostered if code owners get a general endorsement by the EDPB on the code of conduct as such and then invest resources in developing the concrete monitoring scheme. Also it would be possible that code owners want to initate a call for monitoring bodies after having successfully negotiated the code of conduct.

The authors would also like to mention that developing and implementing code specific measures to ensure a rigorous and GDPR compliant monitoring requires ressources from a monitoring body as well. Monitoring bodies may be restrained in investing necessary ressources in the deleopment of a trusted monitoring if it is still in question whether a code of conduct will be approved at all. Such restraints may even be necessary in order to guarantee monitoring bodies' independence by keeping available sufficient financial ressources for their functioning at all times.

To address the abovementioned issues, it might be reasonable to – depending on the content of each individual code of conduct – endorsing a code of conduct by the CompSA and / or EDPB without a accredited monitoring body, if the respective code of conduct includes appropriate content regarding a future monitoring body, that paints a picture of how the respective monitoring shall be put into operation, once the monitoring body gets accredited. Of course, such a code of conduct could only provide the legal benefits if there is a accredited monitoring body in place.

4.5 Monitoring body draft requirements

The Guidelines do not only provide guidance on the requirements to approve a code of conduct, but do also give guidance on the draft requirements, that are to be set out by each CompSA. This approach is helpful as it guarantees that the development of the requirements by different authorities originate from the same starting point.

Nevertheless, some paragraphs raise further questions and need for clarification regarding the development of further requirements for the accreditation.

4.5.1 Consistency between different monitoring bodies

It is highly important to implement the monitoring body as a credible institution, which manages to effectively monitor the compliance with a code of conduct. Under all circumstances, it must be avoided that different monitoring bodies – among each other – start a race to the bottom, with no possibility of national authorities to intervene. This could, as a result, undermine the credibility of the institution *monitoring body* in general. Paragraph 41 of the Guidelines clarifies that the monitoring of a code of conduct can be effectuated by several monitoring bodies:

> *41. (...) A draft code could successfully propose a number of different monitoring mechanisms where there are multiple monitoring bodies to carry out effective oversight.* [Provides mechanisms which will allow for effective oversight (Chapter 6.4)*;* emphasis by authors]

It is very helpful to have the possibility of incorporating multiple monitoring bodies into the code of conduct oversight, e.g. to monitor complex codes, several monitoring bodies can help to guarantee a sufficient monitoring. Nevertheless, having different monitoring bodies in place to monitor the same compliance under the same code of conduct could create the issue of a race to the bottom among the different monitoring bodies. To prevent such a race to the bottom where multiple monitoring bodies are foreseen by a code of conduct, the authors would like to suggest either to require the respective code of conduct to provide an appropriate coherence mechanism, or to clarify that multiple monitoring bodies for one code of conduct can only be approved if they provide different kinds of

monitoring, e.g. concerning different content-related topics, or different levels of compliance. Thereby, it would be assured that the monitoring of a respective code of conduct will not suffer on quality by unreasonable competition between respective monitoring bodies resulting into a race to the bottom.

4.5.2 Information duty of the monitoring body

As mentioned above, some requirements addressed by these Guidelines could be understood in a way that sets out a higher standard than GDPR.

> *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.* [Transparent complaints handling (Chapter 12.5); emphasis by authors]

Without further guidance, this paragraph could be understood in a way that overachieves to a certain extent the legal requirements of Art. 41 (4) p. 2 GDPR.

Art. 41 (4) p. 1 GDPR, on the other hand, as the legal basis of this requirement states:

> *"(...) in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It [the Monitoring Body] shall inform the competent supervisory authority of such actions and the reasons for taking them."* [emphasis by authors]

Therefore, the law only classifies actions taken **against** the code members as worthy of a notification towards the CompSA, not all measures taken in general.

This divergence between GDPR and the Guidelines could lead to different handlings by national competent authorities and thereby to some extent enforce a legal uncertainty and confusion in the market. To not let this fragmentation result in an obstacle for harmonization and standardization of the implementation of codes of conduct, the authors would ask for specification and guidance on this topic, also in the light of Chapter 4.2 *Scope of these Guidelines as a minimum criteria*.

For the sake of completeness, it is indicated that the same point in question is mentioned in paragraph 78:

> *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 is required. 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.* [Communication with the competent supervisory authority (Chapter 12.6); emphasis by authors]

Additionally, some practical guidance on the notification process would be appreciated, e.g. to make the code-specific process of notification of the CompSA (e.g. manner of notification, conditions of notification) subject to the accreditation of the monitoring body as the details may differ depending on the respective code of conduct.

4.5.3 Agreement requirement by the CompSA regarding the monitoring body

Also referring to a possible implementation of higher standards of requirements by these Guidelines, paragraph 79 could create legal uncertainty and fragmentation:

> *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 their 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.* [Communication with the competent supervisory authority (Chapter 12.6); emphasis by authors]

It is understandable and valuable that the CompSA would need notification of the approval, withdrawal or suspension of a monitoring body, to ensure the effectiveness of the code of conduct. As a code of conduct can only be put into operations with a accredited monitoring body, there must be a notification duty if any changes concerning this institution happen, to provide the CompSA with the possibility to react accordingly in a short period of time, if necessary.

As an agreement of the CompSA for such action taken is not explicitly required by law, it seems worthy to reconsider this approach from a practical perspective:

A lack of any provision within a code of conduct requiring such an agreement would not contradict Art 41 (5) GDPR, to the authors' understanding. E.g. if the monitoring body may only be removed for justified reasons, and provided additional safeguards are in place, that either grant a short grace period to replace the monitoring body, or even require a new one to be already appointed, Art. 41 (5) GDPR could also be met. Also, in either way, the new monitoring body would need to be accredited by the CompSA, so there would be no danger of forum-shopping with monitoring bodies.

Therefore, the authors would like to suggest to reconsider this paragraph, taking into account that in order for codes of conduct to get implemented in the market, they will need to be accepted by all relevant stakeholders, also to further encourage them to draw up of codes of conduct intended to contribute to the proper application of GDPR. From the authors' perspective and experience this

cannot, most likely, be achieved by making an agreement with the CompSA mandatory, but by requiring a code of conduct to have safeguards in place if a monitoring body gets suspended or withdrawn from monitoring the code of conduct.

4.5.4 Consequences for a code of conduct in case of revocation of the accreditation

The accreditation of a monitoring body has to have impacts on the monitored code of conduct . As a credible and functioning monitoring is a condition for approving a code of conduct, the absence of such a monitoring must trigger certain safeguards or other mechanisms, that ensure that the monitoring of the code of conduct stays intact. Concerning this issue the Guidelines state:

> *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 by their data subjects or other stakeholders.* [Revocation of a Monitoring Body (Chapter 14); emphasis by authors]

To avoid a fragmentation risk due to different handling in different CompSAs, it would be well appreciated to concretize the margin of discretion opened up by the word *may*. From a practical point of view, a possible concretization could be that a code of conduct shall not be suspended or withdrawn, if the code of conduct itself stipulates a certain appropriate grace period (e.g. 180 days) to find and implement a new monitoring body in cooperation with the CompSA, as they would need to accredit the new monitoring body anyhow. Any automatism of withdrawal or suspension without grace period, though, may manifestly lower the acceptance of codes of conduct in the market. The authors would like to raise the attention to the possibility that a code of conduct may lose its monitoring body not only due to the decision of code owners but also if the monitoring body ceases to exist in law by other means, incl. bankruptcy. In those cases it seems also unreasonable to impose another layer of disadvantages on code owners by automatically withdrawing their legal benefits. However, it should be required that code owners start re-appointing a suitable monitoring body without undue delay and within an appropriate period.

Furthermore, codes of conduct are considered as an element to demonstrate compliance or assess the impact of processing activites. From a practical perspective, it seem worth mentioning, that any automatism of withdrawl or suspension may trigger consequences for those having trusted in the legal certainty of the compliance of the respective code of conduct, even if not declared adherent.

4.5.5 Impartiality of the monitoring body

It is highly appreciated that the Guidelines mark impartiality as one of the main requirements for a monitoring body to be accredited:

> 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 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.* [Independence (Chapter 12.1); emphasis by authors]

Furthermore, the Guidelines divide monitoring bodies into internal or external monitoring bodies.

> 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.* [Independence (Chapter 12.1); emphasis by authors]

It is highly appreciated and welcomed that the undertaken distinction between external and internal monitoring body allows for a flexible arrangement of how the monitoring body will be structure and on the same time, imposes the same level of impartiality as a strict requirement to fulfil for an accreditation.