2 April, 2019

# CISPE Response to the EDPB consultation on draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (the 'Guidance')

## About CISPE

**CISPE (Cloud Infrastructure Service Providers in Europe)** is the primary European trade association representing 30 cloud infrastructure providers operating in Europe, mainly European SMEs headquartered in over 15 Member States. Collectively, they have more than 100 cloud infrastructure services declared under the CISPE Code of Conduct used by millions of businesses across Europe.

CISPE welcomes the draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Such Guidance will not only ease the interpretation of articles 40 and 41 of the General Data Protection Regulation (GDPR) but also encourage a sectorial approach of data protection compliance. By adhering to Codes of Conduct organisations whatever their size can benefit from best practices to address implementation issues raised by GDPR and adopt appropriate governance mechanisms.

Even under the EU Directive 95/46/EC, CISPE has advocated for the development of Codes of Conducts as an efficient instrument of co-regulation in the realm of data protection. In this regard, CISPE has worked closely with Data Protection Authorities since 2016 to develop a Code of Conduct for Cloud Infrastructure Services. Such Code of Conduct aims at providing customers of CISPE members with sufficient assurance that their cloud infrastructure provider is using appropriate data protection standards to protect their personal data consistent with the GDPR.

The CISPE Code of Conduct provides a data protection compliance framework that helps customers of CISPE members to assess whether their cloud infrastructure services can be used to process personal data, and if they will be in compliance with current and future obligations. The Code facilitates the proper application of the new European rules on data protection from the GDPR. CISPE members share the GDPR's objectives of strengthening citizens' fundamental rights in the digital age.

While the recommendations provided by the Guidance are consistent with the CISPE approach, CISPE would encourage the adoption of a clear and simple approval procedure as well as greater clarity over the timeline necessary to obtain such approval. CISPE therefore asks the European Data Protection Board to facilitate efficient coordination between Data Protection Authorities so that Codes of Conduct will be approved under transparent and fixed timelines.

Moreover, we draw the Board's attention to the fact that there is for the moment a low level of maturity in the Monitoring Body market. Certifications Bodies and auditing firms that are best candidates to become Monitoring Bodies, given their skills and auditing expertise, are for the moment hesitating to develop their Monitoring Body offerings. We would therefore encourage guidance to facilitate the take up by these organisations.

This will strengthen the value and efficiency of Codes of Conduct, facilitate compliance of small and medium businesses with GDPR and prove that Codes of Conduct are an innovative way to shift the compliance burden to a more positive approach.

Overall, CISPE is delighted to contribute to the work of the European Data Protection Board and provide insights from a cloud infrastructure provider perspective.

1. **Financial Standing of Monitoring Bodies**

Paragraph 27: *The identified Monitoring Body must have the appropriate standing to meet the requirements of being fully accountable in their role.*
Paragraph 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.*

*a.* CISPE would suggest that further clarity be given as to what the Monitoring Body must demonstrate here: in particular, we would suggest that the Monitoring Body be able to demonstrate sufficient financial standing and financial history in order to give confidence that it can be held financially accountable if that proves necessary in light of the materiality of the role which it is performing.

*b.* CISPE would propose recognition that fines under Article 83(4) will not be imposed on Monitoring Bodies in circumstances where an approved Code sets out a series of objectively defined sanctions and their triggers, and the Monitoring Body has simply followed that set of pre-defined rules. Having a purely objective set of rules for imposition of sanctions will also create certainty for all concerned as to what will happen in the event of non-compliance.

2. **Ensuring efficiency and a level playing field between Monitoring Bodies**

Paragraph 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 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.*

*a.* CISPE would propose that where a Monitoring Body ('MB') is able to demonstrate having used similar mechanisms in practice (i.e. evidence of putting them into practice), rather than just that they are theoretically possible, that this should carry considerable weight in assessing whether a Monitoring Body is suitable

3. **Facilitating the appointment of multiple Monitoring Bodies**

Paragraph 41: *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).*

*a.* We think it is helpful for the potential for multiple MBs to be recognised formally, as this will give options to those who adhere to a Code and facilitate the creation of offerings for the SME market in particular.

*b.* CISPE would propose that where monitoring mechanisms are based on existing standards already employed by a MB (eg. under ISO17065), that this should carry considerable weight in assessing whether those mechanisms are suitable.

## 4. Clarifying approval timelines

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

Paragraph 52: *The CompSA should aim to arrive at a decision within a reasonable period of time, and they should keep the code owners regularly updated on the progress and indicative timelines. They should outline the basis for their 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.*

a. CISPE would ask that the Guidance gives more clarity on meaning of 'reasonable period of time' and 'timely manner'. Some Codes are ready for submission, and we think it is important that these are dealt with quickly now. There is a lack of certainty regarding timeline of process as currently drafted, and it is preferable to set more specific timelines in order to avoid the approval process becoming open ended.

## 5. Clarifying the accreditation procedure for Monitoring Bodies

Paragraph 60: *The CompSA will submit their draft requirements for accreditation of a monitoring body to the Board pursuant to the consistency mechanism referred to in Article 63 of the GDPR.* Paragraph 61 *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.*

*a.* Again, CISPE would ask for more clarity as to the speed with which CompSA draft requirements are dealt with, as this will be a blocker to Code's becoming approved.

b. CISPE suggests that there are standards which already exist which, if adhered to, could form a presumption that the proposed MB meets the requirements of Article 41(2), e.g. ISO 17065 (requirements for bodies certifying products, processes and services); ISO 17020 (requirements for the operation of various types of bodies performing inspection). We note that Article 43(1)(b) GDPR suggests that certification bodies could be accredited with ISO 17065. A similar recognition could be applied to MBs under the Code of Conduct guidance, since there is little substantive difference between the role performed by a certification body, and that performed by a Code MB.

Paragraph 60: *The CompSA will submit their 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.*

c. CISPE understands why this is necessary but would ask for clarity that a Code can be submitted and be considered for approval in parallel with the process of the CompSA seeking approval for accreditation requirements for a MB. Codes should be able to be approved subject to a MB being accredited, provided that there is a proposed MB which has stated its intent to obtain accreditation. Absent this, we are concerned that there will a long timeline associated with having Codes approved since they will have to wait for all other elements to fall into place.

d. For the same reasons, CISPE believes it would be helpful if the Guidance made clear that accreditation requirements for a MB to be submitted by CompSAs can closely reflect what is already set out in the Guidance and are not necessarily expected to set out substantial further detail than does the Guidance.

6. **Clarifying the independence conditions required from Monitoring Bodies**

   Sections 12.1 Independence, 12.2 Conflict of Interest

   a. CISPE proposes that the Guidance suggests that a MB is more likely to be able to demonstrate independence and suitable mechanisms for dealing with conflicts of interest if the MB can show that it has experience with similar issues and has proven mechanisms in place to deal with them.

   b. Again, we would suggest that the Guidance recognises that the ISO standards mentioned above are possible ways to help show sufficient action being taken to deal with these issues/ track record of dealing with these issues.

   c. We would ask that the Guidance be more precise as to how bodies which are connected with the Code itself/ were involved in its creation/ inputted into its drafting, can demonstrate the necessary independence and absence of conflict of interest - for example, specific recognition that individuals involved in Code creation/ drafting should not play a part since they have an intrinsic conflict of interest, requirement that there be no control or influence between individuals who were involved in Code creation/ are responsible for its formation and governance, and those within a MB (eg. rights to hire/fire individuals); presence of full information barriers between individuals involved within MB and those involved in Code itself other than as strictly required for Code administration/ conveying decisions of MB

7. **Reviewing the possibility for Monitoring Bodies to perform random audits**

   Paragraph 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.*

   a. CISPE would ask that the Guidance recognises that random or unannounced audits may not be appropriate as a monitoring mechanism for some Codes, due to the inherent security risks that this would create. For example, cloud services are inherently multi-tenant environments and there is a risk associated with uncontrolled access to those environments.

8. **Clarifying the resource needed by Monitoring Bodies to perform their auditing tasks**

   Paragraph 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.*

   a. CISPE asks that the Guidance should suggest that the MB should be able to demonstrate that it has the capability to scale-up quickly and efficiently without a change in consistency or quality, as it may be difficult to predict with certainty how many members there will be for a code/ how much enforcement activity may be needed. CISPE also suggests that if multiple MBs are available for appointment, this will give more resilience to the monitoring process.

We thank you for your consideration and for the opportunity to submit the enclosed draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (the 'Guidance')

***