Centre for Information Policy Leadership
Hunton Andrews Kurth

29 March 2019

**Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679"**

**Adopted on 12 February 2019**

On 12 February 2019, the European Data Protection Board (EDPB) adopted its Draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (Draft Guidelines).[1] The EDPB invited public comments on this document by 2 April 2019.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments below as input for the EDPB's final Guidelines (Final Guidelines).

## Comments

CIPL welcomes the emphasis of the Draft Guidelines on the added value of Codes of Conduct as a potential means to provide consistent data protection within the European Union, bridging harmonisation gaps between Member States, and as practical, potentially cost effective and meaningful accountability tools.

The GDPR has entered into force almost one year ago and CIPL encourages the EDPB to adopt its Final Guidelines on Codes of Conduct without delay to provide organisations with an efficient tool to accelerate their GDPR implementation efforts. Codes of Conduct are also a mechanism for implementing heightened accountability that goes beyond basic legal requirements and adherence to such schemes should be incentivised by the EDPB and DPAs.[3]

Codes of Conduct are a promising instrument for data protection. As stated in Article 24(3) of the GDPR, Codes of Conduct are intended to serve as an accountability tool that can be used to demonstrate compliance with the GDPR within the EU. Additionally, under Article 40(3) of the GDPR, they can also function as cross-border transfer mechanisms. To achieve these goals, CIPL believes that Codes of Conduct should:

---

[1] Draft Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 74 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] See CIPL white paper on "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

1. Be based on a harmonised EU-wide standard and, preferably, be approved at the EDPB level;
2. Be flexible and scalable to address the needs of companies of all sizes in all sectors or industries, consistent with the mandate of Article 40(1) of the GDPR;
3. Enable interoperability as much as possible with other, similar accountability schemes;
4. Be construed on the basis of a holistic approach which enables both national and/or EU compliance and cross-border compliance; and
5. Take into account the interests of all stakeholders covered by the Codes of Conduct, including data subjects as well as controllers and processors.

Moreover, CIPL underlines that Article 40(1) of the GDPR emphasises that the EDPB, as well as the supervisory authorities (DPAs), should actively encourage the drawing up of Codes of Conduct. Issuing clear and flexible Guidelines that foster the adoption of Codes of Conduct, particularly at the European level, will contribute to this effort.

## I. Codes of Conduct as Accountability Mechanisms

CIPL agrees with the Draft Guidelines that the creation of (sector specific) Codes of Conduct help foster consumer trust, enhance transparency and will contribute to ensuring consistent application of data protection across Europe. CIPL underlines that Codes of Conduct make good accountability mechanisms precisely because of the involvement of industry, in a co-regulatory role, in defining their content. This facilitates the setting up of relevant solutions and best practices for a specific sector as the Code of Conduct is designed to address particular challenges faced by organisations in the relevant sector.

In CIPL's view, the success of Codes of Conduct, as an accountability mechanism, is dependent on the following:

- Firstly, the adoption and approval phase should avoid unnecessary stages of review and bureaucracy. DPAs and the EDPB should be transparent in their review process and with respect to any delays in approval. Uncertainty surrounding the process and timeline for approval may have the negative effect of discouraging organisations from investing their time and resources in drawing up Codes of Conduct. CIPL recommends that the EDPB provide specific guidance on how DPAs and the EDPB should work to provide predictable and expeditious review and approval processes for Codes of Conduct (see further discussion in Section VI below).

- Secondly, CIPL welcomes the fact that the Draft Guidelines place strong focus on the engagement of industry and the representativeness of associations and other bodies that draw up and submit Codes of Conduct (described as code owners in the Draft Guidelines). However, the Draft Guidelines present engagement[4] as a unilateral endeavour of code owners and industry. As Codes of Conduct are co-regulatory mechanisms, CIPL believes that DPAs should also actively engage with code owners and industry (see further discussion in Section VII below).

- Thirdly, the Guidelines should emphasise the general requirement for Codes of Conduct to be calibrated generally to the specific risks of the industry sector for which they are designed. This is fully in line with Article 24(1) of the GDPR which requires the controller to take into account the risks for the rights and freedoms of natural persons when defining and implementing the

[4] *Supra* note 1 at page 19.

appropriate technical and organisational measures to comply with the GDPR. Although the EDPB mentions risk on various occasions, CIPL believes the EDPB should further highlight the integral role of risk assessments in developing and complying with a Code of Conduct. Thus, as risk management is highly contextual in nature and may differ by industry, industry-specific risks should be considered both at the level of drafting the Code and the Code itself should provide for risk assessments by individual organisations that apply the Code to determine the specific risks and relevant mitigations with respect to their own processing operations.

- Fourthly, the creation of diverging requirements between different Codes of Conduct for processors active in multiple sectors and who engage with different controllers in different sectors should be avoided. Otherwise, processors may be bound by various potentially conflicting Codes of Conduct or other accountability tools (such as certifications). It is therefore important that Codes of Conduct are consistent and interoperable with one another as well as with other accountability tools such that compliance with one Code can be leveraged by a processor to satisfy the compliance requirements of another Code.

- Fifthly, code owners should be required to outline the full scope of industries covered by the relevant Code. Where multiple industry sectors are involved, appropriate stakeholders within all the relevant sectors should be involved and the Code should reflect the best practices of all such relevant sectors.

CIPL recommends that the Final Guidelines include a specific section listing the above conditions.

## II. Codes of Conduct and Certifications

Codes of Conduct and certification mechanisms are closely connected. Both are introduced as accountability mechanisms in consecutive articles in the GDPR (Articles 40-41 (Codes of Conduct) and Articles 42-43 (certifications)) and as transfer tools in consecutive sections within Article 46 (see Article 46(2)(e) and (f) GDPR). The procedural aspects of both mechanisms are also similar. For instance, both mechanisms provide for the involvement of a private monitoring entity to deliver a certification (certification body) or to verify that an organisation is compliant with the requirements of a Code of Conduct (monitoring body) in addition to DPA supervision. In addition, Article 64(1) of the GDPR requires that the EDPB issue an opinion where a DPA intends to adopt measures related to both mechanisms.

As co-regulatory mechanisms for the practical implementation of GDPR provisions, both mechanisms should be designed in a consistent and complimentary manner. CIPL regrets that the Draft Guidelines do not address the connection between Codes of Conduct and certifications and urges the EDPB to outline the complimentary nature of both instruments in a separate section of the Final Guidelines.

This would be particularly useful because although certifications are a promising mechanism under the GDPR, the finalisation of the certification framework has been slow, partly due to the complexity of the process chosen to develop them. Almost one year after the GDPR entered into force, not a single certification scheme has been approved by the national DPAs or the EDPB.

The complimentary nature of Codes of Conduct and certifications is in particular evidenced by the following:

- The EDPB appears to have chosen to limit the scope of GDPR certifications to certifying only "processing operations" rather than allowing certification of an organisation's entire privacy

program (as is provided for by Binding Corporate Rules (BCR), for example). As CIPL has previously explained, the GDPR does not compel this narrow scope for certifications and CIPL continues to urge the EDPB to revisit this interpretation. Nevertheless, given this current narrow approach and given that the first initiatives to develop GDPR certifications have been focused on certification at national rather than EU level, Codes of Conduct may act as a substitute mechanism for the restrictive interpretation ascribed to certifications by the EDPB and may serve as useful EU wide mechanisms that cover entire privacy programs across several countries.

- Article 40 of the GDPR provides that the Code may specify the "legitimate interests" pursued by controllers in certain contexts. This would enable Codes of Conduct to be tailored to the specific needs of an industry and to be revised or updated where such needs evolve.

- Codes are flexible tools, which under the GDPR are not necessarily limited to one industrial sector. An example – under Directive 95/46/EC – is the Data Sharing Code of Practice,[5] approved by the UK ICO before the GDPR entered into force. The Final Guidelines should underline this flexibility.

## III. Industry Should Take the Lead in Developing Codes of Conduct

Article 40(2) GDPR places the initiative of preparing Codes of Conduct on associations and other bodies representing categories of controllers or processors (code owners). Whereas the GDPR does not provide further requirements, the Draft Guidelines outline further specifications, in particular with respect to the representation of stakeholders by these code owners. The EDPB sets a high standard on the representativeness of code owners in a given sector.[6] In CIPL's view, this threshold is potentially too high for developing Codes of Conduct and may discourage potential code owners. As such a requirement is not mandated by the GDPR, CIPL recommends the EDPB delete, or at the very least lower, this high threshold requirement.

Instead, it is vital that industry-led organisations prepare Codes of Conduct, which can then serve as mechanisms that can help organisations to demonstrate their accountability and compliance with the GDPR and that can serve as cross-border transfer mechanisms. Industry-led organisations are best placed to produce Codes of Conduct that fulfil the objectives of the GDPR and the EDPB Guidelines while addressing the specific needs of their industry. This is, for instance, relevant where the EDPB recognises that codes can "provide a degree of autonomy and control to controllers and processors and to formulate and agree best practice rules for their given sectors".[7]

It is also important that industry-led organisations be responsible for the review of Codes of Conduct that they helped prepare. The Draft Guidelines currently specify that Codes of Conduct will need to set appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR. As with the development phase, industry-led organisations are best placed to demonstrate whether the Code is working effectively and make any recommendations for changes. Where the proposed changes substantially affect stakeholders not represented by the code

[5] UK ICO, Data Sharing Code of Practice, May 2011, available at https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.
[6] *Supra* note 1 page 10.
[7] *Id*. at page 8.

owner, the views of these other stakeholders should also be taken into account before the changes are implemented in a revised Code of Conduct.

CIPL underlines, therefore, that industry should take the lead in developing and reviewing Codes of Conduct. The consultation with stakeholders, as foreseen in the Draft Guidelines,[8] could be a good way to involve interested companies that are not represented by an association that drives a Code. It also provides a method to involve stakeholders outside of the industry in the process (e.g. civil society, ethics experts where relevant). The Final Guidelines should highlight this point.

In addition, the Final Guidelines should provide further clarity on the definition of "code owners" and, in particular, on "interest groups". The Draft Guidelines define code owners as the association/consortium of associations or other bodies representing categories of controllers and processors including trade associations, sectoral organisations and interest groups.[9] In particular, the Final Guidelines should specify whether "interest groups" would also include groups created via private initiatives of multi-stakeholders without the involvement of trade/industry associations. In any case, they should also specify that the views of all stakeholders impacted, including of the industry, must be taken into account at the early stages of the drafting and review process of Codes of Conduct.

## IV. Codes of Conduct in a Transnational Context

The Draft Guidelines distinguish three different situations with respect to the geographic scope of Codes of Conduct: (1) national Codes, (2) transnational Codes and (3) Codes covering cross-border processing.

CIPL supports the EDPB's creative approach that allows for the adoption of transnational Codes in cases where there is no cross-border processing as defined by Article 4(23) of the GDPR. In other words, a Code can be valid in more than one Member State, even if it covers national data processing, without being subject to the cooperation mechanism of Articles 56 and 60 of the GDPR. The approval of such a transnational Code of Conduct takes place on the basis of "sui generis" DPA cooperation, with a "chosen DPA" and a procedure for other DPAs to act as co-reviewers.[10] This cooperation procedure appears similar to the BCR approval procedure.

CIPL believes that this approach has the advantage of preventing the unnecessary fragmentation of Codes. In addition, it may be the case that a code owner could want to have a successful national Code submitted for transnational approval. It would be useful if the Final Guidelines encouraged this, specifying the procedure to be followed.

Unfortunately, the Guidelines only mention that decisions and communications to code owners in the proposed cooperation procedure be "timely", without clarifying what this means in practice.[11] The Final Guidelines must provide for more precise timelines for the review and approval of Codes, which should not be longer than strictly necessary. This would enhance the effectiveness and the EU wide consistency of the procedures, as well as legal certainty for organisations and better resource management.

Finally, CIPL recommends the EDPB clearly express a preference for EU wide Codes of Conduct and commit to ensuring an efficient and timely review to avoid unnecessary further delays in the adoption of a Code.

---

[8] *Id*. at page 11.
[9] *Id*. at page 10.
[10] *Id*. at pages 17-19.
[11] *Id*. at page 18.

## V. Codes of Conduct as Transfer Mechanisms

Approved Codes of Conduct, together with binding and enforceable commitments of the controller or processor, are recognised as transfer mechanisms under Article 46(2)(e) of the GDPR.

According to the Draft Guidelines, the EDPB plans to issue separate guidelines on Codes of Conduct as transfer mechanisms.[12] It is important that Codes of Conduct are developed with a view to facilitating the transfer or personal data and CIPL emphasises the importance of issuing such guidance without delay, highlighting Codes as a further mechanism in the data flow toolbox for controllers and processors when considering cross-border data transfers. In practice, this should mean that a company participating in a Code of Conduct should also be able to use the Code as a basis for data transfers and should not have to be subject to a different Code for transfer, although, obviously, the transfer itself may require additional safeguards.

There is a close connection between Codes of Conduct and other transfer mechanisms, in particular with approved certification mechanisms set forth in Article 46(2)(f) of the GDPR. CIPL highlights the relevance of this relationship and the need to have similar approaches in defining "binding and enforceable commitments". CIPL recommends looking at existing instruments to define these commitments, including those set up by companies with approved BCR who have the obligation to make these BCR applicable and enforceable internally (in the case of controller BCR) and externally (in the case of processor BCR).

CIPL notes that the EDPB also plans to issue guidelines on certifications as transfer tools. It would make sense for the EDPB to consider merging the guidance on certifications and Codes as transfer tools into one set of guidelines. Even more importantly, the guidelines relating to both these transfer mechanisms should be fully consistent with each other and drafted with a view to encouraging the availability of both mechanisms for controllers and processors, in an effective and scalable manner.

## VI. Approval of Codes of Conduct

Article 40(5) of the GDPR requires that a DPA provide an opinion on a draft Code of Conduct submitted to it (see further discussion in Section VII below) and that it shall approve the Code if it finds that it provides sufficient appropriate safeguards. This is a simple and clear duty.

However, the Draft Guidelines add an additional criterion for the approval of Codes of Conduct. In particular, they require that code owners demonstrate the need for establishing a Code of Conduct.[13] This is a requirement that appears to go beyond the mandate of the GDPR, because the GDPR clearly states that in case of sufficient appropriate safeguards, a Code shall be approved. In any event, CIPL believes that DPAs are not necessarily best placed to assess whether a Code of Conduct meets the specific needs of a sector. This assessment should be made by the code owners.

In terms of the content of a Code and how it should be assessed by the DPA, CIPL agrees that a Code should specify the application of the GDPR[14] and not merely restate its provisions. CIPL also strongly encourages including examples and best practices in a Code. However, Codes of Conduct should not necessarily always provide operational meaning to all principles under Article 5 of the GDPR. The text of the Guidelines could be more nuanced and allow for appropriate flexibility in this respect.

---

[12] *Id*. at page 5.
[13] *Id*. at page 13.
[14] *Id*. at page 14.

Furthermore, Recital 98 of the GDPR states that Codes of Conduct should be drawn up so as to facilitate the effective application of the GDPR. While CIPL agrees with this objective, this should not be translated into a requirement that each Code of Conduct should provide "clear industry specific improvements in terms of compliance".[15] This might discourage the proposing of Codes of Conduct.

Finally, CIPL understands that Codes of Conduct that existed before the entry into force of the GDPR need to be reassessed in light of the substantive changes brought about by the Regulation.[16] However, CIPL recommends the EDPB specify in its Final Guidelines that the review of existing Codes does not necessarily require a full re-evaluation. Any re-evaluation should be limited to elements of data protection law that essentially changed with the GDPR.

## VII. Engagement of DPAs

The Draft Guidelines contain a section on engagement,[17] formulating engagement mainly as a duty for code owners to engage with DPAs. In CIPL's view, however, engagement should express a mutual willingness of involved partners, including DPAs, to engage in a constructive manner with stakeholders. As explained in CIPL's white paper on Regulating for Results – Strategies and Priorities for Leadership and Engagement,[18] "[…] this brings to life Article 57(1)(d) of the GDPR which implicitly recognises that both sides could do much to assist the other to bring about optimum regulatory outcomes".

The approval of Codes of Conduct is a logical area where mutual engagement would add value. Particularly, it should be clarified in the Final Guidelines that the procedure in Article 40(5) of the GDPR which requires a DPA to provide an opinion on a Code of Conduct should be informed through engagement and a consultation process with the relevant applicant to address and resolve any issues with respect to the Code prior to approval.

CIPL recommends including this approach in the Final guidelines. Engagement should be presented as mutual engagement.

## VIII. Monitoring of Codes of Conduct

Monitoring is and should be a core element of Codes of Conduct. This is also illustrated by Article 41 of the GDPR. It is therefore logical that the Draft Guidelines provide further details on the monitoring of Codes of Conduct, including the role of monitoring bodies.[19] The EDPB accepts that code owners can choose an internal monitoring body, provided that these bodies operate with a sufficient level of independence.[20] CIPL supports this flexibility and understands that this raises issues of independence which should be sufficiently addressed, in line with Article 41(2)(a) of the GDPR.

Monitoring bodies should be accredited by DPAs as per Article 41(2) of the GDPR. Accreditation is not part of a DPA's usual tasks. It is also mentioned in the context of Article 43 of the GDPR on certifications, albeit in a different manner. CIPL is aware of this difference which cannot be remedied by the EDPB.

---

[15] *Id*. at page 14.
[16] *Id*. at page 5.
[17] *Id*. at page 19.
[18] "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf.
[19] *Supra* note 1 at page 6-7.
[20] *Id.* at pages 20-21.

However, to ensure consistent and effective application of the GDPR, CIPL recommends that DPAs align their approaches as much as possible with the approach taken in the area of certification.

In addition, CIPL suggests the following points be reflected in the Final Guidelines:

- The Draft Guidelines require that monitoring bodies identify risks to independence on an ongoing basis.[21] CIPL recommends that the EDPB elaborate on this, for instance, by recommending certain methodologies or professional standards in consultation with relevant stakeholders, such as potential monitoring bodies.

- The Draft Guidelines state that a monitoring body will have to establish transparent complaint-handling mechanisms.[22] The Final Guidelines should:

    - Specify that transparency and due process are core principles of complaint handling carried out by monitoring bodies; and
    - Explain how such mechanisms interact with complaints submitted to DPAs under Article 77 of the GDPR.

- The Draft Guidelines state that monitoring bodies can be internal or external. The Final Guidelines should provide more clarity on this point, in particular:

    - Whether internal and external monitoring bodies could co-exist;
    - Whether internal and external monitoring bodies would have different responsibilities and how they would work together (e.g. on the basis of a cooperation mechanism in order to allow internal monitoring bodies to opine on enforcement measures before they are issued by external monitoring bodies and vice versa);
    - Whether monitoring bodies of Codes of Conduct that have overlapping elements should cooperate to ensure consistency of enforcement;
    - Whether it would be possible to outsource activities of internal monitoring bodies;
    - Whether the Data Protection Officer could exercise the role of an internal monitoring body;
    - Whether members could be exempt from enforcement of the external monitoring body if they assign an internal monitoring body; and
    - Under what circumstances members could assign internal monitoring bodies.

## IX. Codes of Conduct and Sanctions

CIPL wishes to raise the issue of compliance with a Code of Conduct to mitigate possible sanctions. The Draft Guidelines only mention that adherence to a Code is a "factor taken into consideration" by a DPA.[23] CIPL recommends that this statement be revised to explicitly state that compliance with Codes of Conduct can be used as a mitigating factor.[24]

---

[21] *Id*. at page 20.
[22] *Id*. at page 22.
[23] *Id*. at page 9.
[24] This is in line with CIPL's previous comments on the EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, 10 July 2018, available at

**Conclusion**

CIPL is grateful for the opportunity to provide comments on key implementation questions on codes of conduct and monitoring bodies in accordance with Articles 40 and 41 GDPR. We look forward to providing further input as the Guidelines are finalised, as well as to contributing generally to the development of effective, interoperable and scalable Codes of Conduct that can also serve as data transfer tools under the GDPR.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_edpb_draft_certification_guidelines__10_july_2018_-c.pdf at page 9.