ASSOGESTIONI
associazione del risparmio gestito

Rome, 1 April 2019

EDPB – European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
Belgium

Our ref: 77/19

Sent by email at EDPB@edpb.europa.eu as required by the Consultation

Assogestioni's reply to the EDPB's Consultation on Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

Assogestioni[1], the representative association of the Italian investment management industry (hereinafter the Association), welcomes the opportunity to reply to the EDPB's Consultation on Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Our members are indeed particularly interested in the rules on Codes of Conduct and Monitoring Bodies, given that the Association created a Task Force among its members that drafted a code of conduct.

First of all, we would like to express our appreciation for the work carried out by the EDPB: the choice of introducing the Guidelines is highly sensible and it would provide a clearer framework for market participants, while contributing to foster convergence across Europe with reference to this part of the rules of the GDPR.

Whilst the Guidelines cover several topics, our comment will be focused on a single issue that is considered of the utmost importance by our members.

This issue is that the Guidelines prescribe that the codes of conduct must identify a monitoring body which has to be accredited by the Competent Supervisory Authority to control the compliance with the code itself.

Our comment to the abovementioned prescription of the Guidelines is threefold.

1) First, the aforesaid prescription seems to be in conflict with the rules provided by the GDPR. Please consider that Article 41(1) of the GDPR provides that "(…) *the monitoring of compliance with a code of conduct pursuant to Article 40* ***may*** *be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority*". On the other hand, the Guidelines, for example in paragraph 60, provide that: "*In order for a code (national or transnational) to be approved, a*

[1] Assogestioni represents the interest of the Italian fund and asset management industry. Its members manage funds and discretionary mandates around EUR 2.000 billion (as of December 31st, 2018).

*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*". The two provisions just reported above seem to be in sharp contrast: while the GDPR provides for a possibility, the Guidelines provide for an obligation[2]. The Guidelines declare that their aim is to provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR, but in this case we have the impression that the Guidelines are going beyond their aim by setting a provision that is in contrast with the text of the GDPR.

In this respect we have also considered that the GDPR, in Article 40(4), provides that a code of conduct shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it. In our opinion, however, the "mandatory monitoring" prescribed in Article 40(4) cannot be interpreted without taking into consideration that Article 41(1) merely envisages the possibility (not the obligation) to identify a monitoring body. In our view, the correct interpretation of the aforesaid provision expressed in Article 40(4) is that, in case a monitoring body is identified within a code of conduct, the code must also provide for mechanisms which enable that body to carry out the monitoring that it is tasked to perform by the GDPR. To be more precise, Article 40(4) prescribes a mandatory monitoring, but it cannot be interpreted in the sense that this activity should always be performed by a monitoring body, because such an interpretation would totally disregard the text of Article 41(1) which - again - provides for the possibility (not the obligation) to identify a monitoring body. The mandatory monitoring might be entrusted, for instance, to other functions already existing (e.g. the Compliance Department or the DPO).

2) Second, a rule demanding the appointment of a monitoring body implies a possible duplication of controls. Article 39 of the GDPR provides that a DPO is charged, *inter alia*, with the task "*(…) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data (…)*". This provision, in our view, implies that a DPO could not refrain from monitoring the compliance with a code of conduct, in case the controller or the processor undertook to apply it. Therefore, in the cases where a DPO is designated, the appointment of a monitoring body would result in an additional control to that one already done by the DPO. For this reason, as suggested above, in cases where the monitoring body would not be identified, the DPO could be viewed as a function that can be entrusted with the duty to perform the mandatory monitoring according to Article 40(4).

3) Third, we would draw the attention on the circumstance that a provision demanding the identification of a monitoring body, instead of encouraging the drafting of codes of conduct, as required by Article 40(1) of the GDPR, might hamper their drafting in many specific sectors. The requirements set by the Guidelines for the accreditation of monitoring bodies allow to think that, in fact, it would be difficult that a monitoring body will be established within a code owner, but it seems also difficult

[2] The obligation to identify a monitoring body is prescribed in various parts of the Guidelines.

that external monitoring bodies may emerge. This opinion is based on the following reasons.

In the first case (i.e. the case of an internal monitoring body) the need to comply with the requirements of independence and absence of conflicts of interest in relation to a code owner would be expensive. Indeed, the establishment of an internal monitoring body would involve the creation of separate offices and a dedicated staff with an adequate operational experience and training within a code owner. Moreover, it would also entail a risk, since the body can be fined as per Article 83(4)(c).

In the second case (i.e. the case of an external monitoring body) the establishment of an organization that implies costs and risks is again required, and it is not clear how (for instance) the costs could be covered without jeopardizing the independence and the absence of conflicts of interest (for example, the funding through contributions paid by the members of the code seems to contrast with the need to maintain these two requirements).

In a nutshell, we do not want to say that monitoring bodies would be appointed hardly because of the costs and risks that their creation entails. We want to say that, since the creation of monitoring bodies implies costs and risks, it should be required only in those cases where it is necessary (e.g. because the code of conduct is conceived to be applied to a "high risk" sector), and/or within specific sectors that are able to cope with those costs and risks.

In conclusion, we believe that the three reasons outlined above (if the appointment of monitoring bodies would be always required in order for a code to be approved) may prevent many associations to develop a code of conduct. Therefore, in the light of the considerations made above, we believe that it would be valuable if the EDPB would reconsider those parts of the Guidelines which require that the codes of conduct must identify a monitoring body.

Should you have any queries, please do not hesitate to contact us.

Yours faithfully,

The Director General