ESOMAR, FEDMA, EFAMRO joint statement on Guidelines 04/2021 on codes of conduct as tools for transfers by the European Data Protection Board.

October 1st 2021

This statement is co-signed by ESOMAR, FEDMA and EFAMRO without prejudice to any additional individual statement that might be submitted by the respective organizations and which we recommend to keep into consideration.

With this statement, we wish to thank the European Data Protection Board for the opportunity to provide our comments to the Guidelines 04/2021 on codes of conduct as tools for transfers of personal data (hereinafter the "Guidelines").

As an initial remark, ESOMAR, FEDMA and EFAMRO wish to welcome and support EDPB's intention of providing, through the Guidelines, practical guidance for code owners, for codes that are amended and/or expanded in their scope with a view to also being used as a tool for transfers.

We believe that the Guidelines have the potential to streamline the procedures involved in the assessment process, however further clarification is sought on the general validity mechanism and, on the criteria, to determine what supervisory authority will be competent to accredit the monitoring body, e.g. paragraph 19 of the Guidelines.

We wish to underline to the European Data Protection Board that currently many market players consider compliance to the GDPR as significantly impacting their business operations. They view Codes of Conducts often as additional burdens unless Code owners demonstrate business benefits to sign up to them. Many of our members have indicated, for example, that it is their ability to facilitate cross border work with other business partners that makes the Code useful and interesting for them to sign up to. For some sectors, and therefore some Code owners, the project is only viable when these aspects are reasonably certain to be approved provided, they meet the requirements established by the EDPB.

Considering the above, we wish to formulate the following recommendations:

1. **Streamline processes as much as possible**

As provided by paragraph 21 of the Guidelines "[...] *the Commission may decide by adopting an implementing act that a code intended for transfers and approved by an SA has general validity. Only those codes having been granted general validity within the Union may be relied upon for framing transfers*".

However, when referring to Articles 40(3) and 40(9) GDPR we note that the general validity mechanism as an implementing act as well as its related legal effects remain generally unclear. Thus, additional guidance within the Guidelines would be appreciated on how the general validity mechanism will be implemented by the European stakeholders aside the EDPB.

In this respect, we believe that the substantive assessment of the candidate code of conduct, including its dimensions for safe international transfer, should be made by the EDPB and the European Commission simultaneously as part of a single procedure, rather than having to face a doubling of the procedures that may further discourage candidates from considering codes of conduct. We also believe ultimately this would improve efficiency and prevent undue delays in the process of granting general validity and safeguarding a sector's interest. This will ultimately allow for a more rapid and enthusiastic international adoption of these tools by any given sector.

Moreover, as some Codes are already in various stages of the approval process, we believe it may be appropriate to adopt an appropriate transition period to reduce uncertainty for those already in a process prior to the final adoption of these guidelines.

Notwithstanding and in full appreciation of the powers of the European Commission, procedures by the European Commission should not – by any means – foresee any timelines that exceed the suitable blueprint provided by Article 40 GDPR related to the processes to be performed by the EDPB, i.e., a default period of eight weeks plus an optional extension in case of need, e.g., due to complexity of the case.

2. General validity should not always be required

With regard to paragraph 21 of the Guidelines, we wish to note that if read in conjunction with Article 40(3) of the GDPR, the Guidelines' text seems to create the impression that safeguarding codes of conduct need a general validity in any case. The Guidelines provide that safeguarding codes of conduct may be signed either by EEA companies, non-EEA companies or even both. Especially, if the scope of a Code only foresees EEA companies to adhere to, the requirement of a general validity appears excessive. We recommend that the Guidelines should be clarified and further aligned with Art. 40(3) GDPR and that the general validity mechanism provided for in this Article must not be applied to codes of conduct not concerning third-country transfers.

3. Clarify processes and requirements for monitoring bodies

We refer to the GDPR's original ambitions, which is to foster the creation of a Digital Single Market, part of the essential mechanisms of this is of course the One-Stop-Shop and the establishment of single points of contacts for legal persons under the GDPR. We are convinced that extending this principle to the monitoring body would enable further progress towards this ambition. It also ensures that the monitoring body can develop and further its activities informed by a close relationship to a singular Supervising Authority (i.e. lead authority or local authority) rather than having the difficulties of potentially managing diverging requirements from multiple Supervising Authorities. Noting once again, that the appetite for Codes of Conducts maybe not always be guaranteed, we believe all measures to simplify procedures will further enhance the attractiveness of this compliance tool (and ultimately their efficacy once deployed across more sectors).

As foreseen by paragraphs 17, 18 and 19 of the Guidelines, code owners can identify a monitoring body, which will need to be accredited by the competent supervisory authority in line with article 41 GDPR, whose role will be to monitor that third country controllers/processors having adhered to such code comply with the rules set out in the code.

In this regard, we observe that if the code owner delegates the monitoring of the code to an entity within the EEA, it is unclear what the criteria will be to determine what supervisory authority will be competent to accredit the monitoring body, as monitoring requirements, while being substantially high, might vary among member states.

We believe that monitoring body requirements should be tailored to the code of conduct, its sector and the data processing risks and therefore we wish to recommend that the supervisory authority competent for the accreditation of the monitoring body is the data protection authority that has jurisdiction where the monitoring body is established. We believe that this will encourage not only platforms but also European SMEs to develop codes with monitoring systems adapted to their sector and their processing of data.

Contact details:

ESOMAR

Address: Atlas Arena, Azië building - 5th floor
Hoogoorddreef 5, 1101 BA Amsterdam, Netherlands
Telephone: +31 20 664 2141- Fax +31 20 664 2922
Email: public.affairs@esomar.org
Website https://www.esomar.org

FEDMA

Address: Avenue des Arts, 43. BE-1040 Brussels, Belgium
Telephone: +32 2 779 4268 - Fax: +32 2 778 9922
Email: info@fedma.org
Website: https://www.fedma.org

EFAMRO

Address: Bastion Tower, level 20
Place du Champ de Mars 5
B-1050 Brussels, Belgium
Telephone: +32 (0)2 550 3548 - Fax: +32 (0)2 550 3584
Email: info@efamro.eu
Website: https://efamro.eu