27/06/2022 Position Paper

EFAMRO and ESOMAR Consultation Response

A Response to the draft EDPB Guidelines on the calculation of administrative fines under the GDPR

This paper is submitted on behalf of:

EFAMRO the European Federation of Associations of Market Research Organisations. Founded in 1992, EFAMRO represents the interests of market, opinion and social research in Europe. Its members are national trade associations for research businesses.[1]

ESOMAR the global voice of the data, research and insights community since 1947, it promotes the value of market, opinion and social research and data analytics.[2]

1. About Market, Opinion and Social Research

1.1. EFAMRO and ESOMAR represent the data, research and insights sector, accounting for in Europe a reported annual turnover of €20.87 billion.[3]

1.2. Market, opinion and social research is the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to gain insight or support decision making. It involves systematic study of different spheres of society, politics, and the economy. Research, insight and analytics stand at the heart of all well-informed commercial, social and political decisions. Insight into what makes a product, business initiative or government policy work is often the hidden – yet defining – factor between success and failure. It is our sector that provides the deeper intelligence needed for our world today.

1.3. Many research and analytics providers subscribe to established self-regulation schemes that enable research respondents and participants to enforce their rights. These are built on established international standards set forth by the ICC/ESOMAR International Code and national codes across many EU countries[4].

2. Purpose of our Response

2.1. Our associations are responding to the European Data Protection Board's (EDPB's) proposed *Guidelines -04/2022 on the calculation of administrative fines under the GDPR,* which sets out plans to harmonise the methodology supervisory authorities use when calculating of the amount of the fine.

[1] For more about EFAMRO see: https://efamro.eu/
[2] For more about ESOMAR see: https://esomar.org
[3] ESOMAR Global Market Research Report, which includes contributions from national associations including EFAMRO members: https://esomar.org/global-market-research-report
[4] ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics: https://esomar.org/code-and-guidelines/icc-esomar-code

2.2. Our associations largely support and welcome the guidance. We do however have some concerns about breaches to the supply chain and the calculation of fees where there is shared liability.

3. Detailed Feedback

Breaches to the supply chain

[Page 11] One sanctionable conduct

3.1. We recommend including a provision that takes account of breaches to the supply chain, and in such cases identify which party carries the larger share of responsibility. The nature of market, opinion and social research activities can result in supply chains which involve a number of different processors. For example, activities such as translations, transcriptions, data processing, scripting, data collection, etc are often outsourced and fieldwork is frequently outsourced to third-party sources. Presently the guidance does not cover detail on shared liabilities, and the responsibility of said liabilities beyond the controller and processor. As such, where a party is responsible for bearing part of the risk in any activity, which party absorbs the larger share or how are the fines divided across the supply chain? How does this impact concurrence of offences - where it may be unlawful to sanction multiple offenders, where there is shared liability, more than once?

[Page 18] Intentional or negligent character of the infringement

3.2. Chapter 4 contains some helpful and clear guidance about categorisation and seriousness of infringements. It would be helpful if there was more detail about a processor responsibility if they were to undertake illegal processing, unaware that it was such, due to misleading instructions from a controller. Would the processor be held responsible for not identifying misleading instructions? And if so to what degree? The inclusion of an example covering this type of scenario would be helpful.

[Page 25] Degree of responsibility of the controller or processor

3.3. We recommend providing more clarity, context and examples of the division of responsibility between the controller or processor/s, and the overall supply chain. It would be helpful if examples could be given to contextualise clause 78 and 82:

Following Article 83(2)(d), the degree of responsibility of the controller or processor will have to be assessed, taking into account measures implemented by them pursuant to Articles 25 and 32 GDPR. In line with Guidelines WP253, "the question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation."

"Given the increased level of accountability under the GDPR in comparison with 95/46/EC it is likely that the degrees of responsibility of the controller or processor will be considered an aggravating or a neutral factor. Only in exceptional circumstances where the controller or processor has gone above and beyond the obligations imposed upon them, will this be considered a mitigating factor."

For example, where there is a complex supply chain and a party within the chain fails to adequately meet their responsibilities, i.e., in a research project, if translation is outsourced and the party misrepresents or misuses a tranche of data - this could have a direct impact on the data that is used by other parties in the supply chain. In such a case, is the onus of a breach across the chain with the party that broke protocol (in this case the translators)? Ultimately, how would the degree of responsibility be determined for a range of data processors involved in a complex supply chain where processors might only have a partial view of the activities?

[Page 29]: Adherence to approved codes of conduct or approved certification mechanisms

3.4. We appreciate the guidance on the approved codes of conduct or approved certification mechanisms including the recognition that adherence to these may in "some circumstances" constitute a mitigating factor. We also welcome clause 106 which states that failure to comply with the codes of conduct or certification may be considered an aggravating circumstance. We recommend that supporting approved codes of conduct should always be a recognised as a mitigating factor when considering fines. This section of the guidance. However, In light of the investments needed from both code owners and code signatories and to encourage the further adoption of code of conducts and other certified mechanisms, we do believe that adherence to these tools should represent a constant mitigating factor. We also believe that a similar provision would ensure an harmonized interpretation of the Guidelines amongst different supervisory authorities.

3.5. We therefore recommend the following amendment to clause 105 of the Guidelines:

> 105. As recalled by Guidelines WP253, adherence to codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR ~~may in some circumstances~~ constitutes a mitigating factor. Approved codes of conduct will, according to Article 40(4) GDPR, contain "mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions." Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to Article 41(4) GDPR, including suspension or exclusion of the controller or processor concerned from the code community. Although the supervisory authority can take into account previously imposed sanctions pertaining to the self-regulatory scheme, the powers of the monitoring body are "without prejudice to the tasks and powers of the competent supervisory authority", which means that the supervisory authority is not under an obligation to take into account any sanctions by the monitoring body.

4. Minor observations

4.1. There are segments of the guidance which are quite complex and inaccessible to those without specialist knowledge, chapter 3 in particular. The addition of further practical examples would help to make the guidance more accessible and reduce the cognitive burden for readers of the document.

4.2. There are some typos which need to be addressed: and there are some footnote references, 11 and 12 on page 13, which need to be added.

5. Implications to the sector

5.1. Overall, we welcome the creation of the Guidance. However, providing more clarity and explicit provisions around the concerns raised could be addressed in the final version of the Guidance which should support understanding and adherence to the Guidance.

6. Next Steps

6.1. EFAMRO and ESOMAR welcome the opportunity to assist the EDPB in updating and finalising the Guidance. To contact us for more information:

- Kaleke Kolawole, Head of Policy: kaleke.kolawole@efamro.eu
- Claudio Gennaro, Senior Advocacy Programmes Coordinator: claudio.gennaro@esomar.org