Guidelines 04/2022 on the calculation of administrative fines

Joint Comments by SRIW and SCOPE Europe

June 2022

1 About the Authors

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: "**SRIW**") is a Berlin-based non-profit-organisation that fosters and promotes data and consumer protection through self-regulation and co-regulation. Its Brussels-based subsidiary SCOPE Europe sprl / bvba ("**SCOPE Europe**") complements the portfolio of **SRIW** on a European level and is an organisation supporting credible and effective co-regulation of the information economy. It acts as a think tank to debate key issues in digital policy and provides an umbrella organisation for a range of co-regulatory measures in the digital industry. SCOPE Europe was founded in February 2017 and acts as the secretariat and accredited independent Monitoring Body of the EU Data Protection Code of Conduct for Cloud Service Providers (the "**EU Cloud Code of Conduct**") pursuant to Article 41 GDPR.

SRIW and SCOPE Europe are calling for suitable regulatory methods to foster innovation and drive the digital transition while promoting corporate responsibility, particularly in the fields of data protection. To achieve this overarching objective, SRIW and SCOPE Europe work to enhance transparency and strengthen best practices in data protection by mobilising and supporting the industry to engage in binding voluntary commitments underpinned by appropriate sanctions such as codes of conduct. In this context, SRIW and SCOPE Europe ("**We**") appreciate the opportunity to submit this comment in support of the Guidelines.

2 Preliminary Note

We would like to thank the EDPB for granting stakeholders the opportunity to provide their feedback on new guidance as well as for past projects. **We consider the Guidelines to be an essential piece of orientation**, as fostering harmonization in the methodology used by supervisory authorities to calculate fines is essential to ensure that key administrative and democratic principles such as predictability and legal certainty are maintained.

The comments that will follow have been drafted from our viewpoint as organisations that specialise in the development and monitoring of codes of conduct based on Articles 40 and 41 GDPR.

Our comments follow a twofold structure. Firstly, we will begin with high-level overall observations. Secondly, we will provide more detailed remarks that centre around the mitigating aspect of adherence to codes of conduct as well as the applicability of the Guidelines to Article 41 accredited monitoring bodies.

3 General Remarks

SCOPE Europe and SRIW greatly appreciate that the guidelines refer to the fact that adherence to codes of conduct (pursuant to Article 40 of the GDPR) or approved certification schemes (pursuant to Article 42) may be a **mitigating and relevant factor in the decision on whether to impose a fine as well as on the respective amount of such administrative fine**. In this regard, we welcome the reinforcement of legal benefits of these instruments. **Nonetheless, we believe that there are still some important elements that have not yet been covered, while others need further clarification**.

Against this background, we must recommend that references made to the legal benefits of codes of conduct are made clearer and more detailed. We find that such amendments shall be crucial for the **correct interpretation of the objective and advantages of adhering to these tools**.

In this regard, while we fully acknowledge that the established monitoring system does not negate the powers of the authorities, the legal benefits of adhering to a code of conduct should be very well reflected throughout the Guidelines. This is particularly relevant considering that GDPR's intent is to meaningfully encourage the development of such tools and, consequently, to **establish incentives to facilitate as well as disseminate its implementation**.

Finally, **further guidance is welcome on the applicability of the criteria established by the Guidance in the context of accredited monitoring bodies.** A direct application of the Guidelines towards monitoring bodies might negatively affect their role under GDPR, especially when it comes to having the (general) turnover as a reference point.

3.1 Mitigating Aspect of Adherence to Approved Codes of Conduct

As exposed above, **it is the intent of GDPR that adherence to an approved code of conduct provides legal certainty and, in turn, yields some mitigating aspects when sanctions are imposed**. Therefore, regarding the legal benefits of adhering to an approved GDPR code of conduct, SCOPE Europe and SRIW believe that **the following aspects should be taken into consideration and further emphasized in the Guidelines.**

We recommend that the guidelines further reflect, Article 83 (2) GDPR which states that "*when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to (...) adherence to approved codes of conduct pursuant to Article 40*".

In this respect, **Art 41.4 GDPR** states that "*without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a Monitoring Body shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code*"[1].

One can then understand that the action taken by a monitoring body does not restrict a competent supervisory authority to act on a later stage. Therefore, a company can be sanctioned for the same infringement by a monitoring body and by the competent supervisory authority.

In this context, the competent supervisory authority can fine on its ground a company which has been already sanctioned by a monitoring body for the same infringement, but when a supervisory authority assigns a penalty, it shall **take into consideration whether the company is adherent to a code of conduct and if measures and sanctions has already been taken by the monitoring body**.

Consequently, adherence to a code of conduct is a factor to be considered when a competent supervisory authority decides to impose a fine. Following the abovementioned elements, **such consideration, shall not be solely focused on the aggravating factor**, such as currently stated in the Guidelines.

On the contrary, we understand that many, if not most, companies that choose to adhere to a code of conduct will not intentionally and deliberately or due to a gross negligence infringe a code – and GDPR. Therefore, **we believe the establishment of fines shall be layered according to the following likely scenarios to emerge:**

1- Shall an infringement be a result of a non-communicated new interpretation of the law by the supervisory authority, which has not been aligned with the requirements of an approved code, by default no fine shall apply.
2- Shall an infringement be a result of an unintentional/non-abusive negligence, the supervisory authority, in accordance with Article 83 (2) GDPR, shall by default consider the voluntarily adherence to an approved code of conduct as a mitigating factor.
3- Shall an infringement be a result of a gross/abusive negligence, the supervisory authority shall by default consider the voluntarily adherence to an approved code of conduct as an aggravating factor.

[1] Article 41.4 GDPR.

We believe that such staggered approach would reflect well the requirements of GDPR while guaranteeing that incentives are properly in place for companies to adhere to codes of conduct – and by that to voluntarily subject themselves to additional compliance safeguards/efforts.

Ad 1: In cases where a controller or processor is adherent and compliant with a code of conduct, and the potentially infringing behaviour solely concerns the scope of such code of conduct, the guidelines shall clarify that by default there shall be no administrative fine. Especially, where a code of conduct may be very precise in its requirements. Given the intense involvement of supervisory authorities in the approval process, adherent controllers and processors should be provided with a significant trust of stable interpretation of the law.

This shall not – by no means – limit the powers of supervisory authorities. Nor shall it overrule the direct applicability of potentially conflicting court decisions. However, code-owners and monitoring bodies are required to constantly review a code of conduct and ensure it remains compliant with GDPR. As the scenario of disclosing a modified interpretation by a supervisory authority without previous request to the code-owners to adapt the requirements in due time – or following a change of law or recent court decisions – is unlikely, such a clarification to the Guidelines will provide the necessary legal certainty without doing any harm.

Ad 2: In cases, where codes of conduct will allow for different interpretations or means of implementation, the Guidelines should clarify that by default adherence to a code of conduct shall be considered positively, i.e., as a mitigating factor. Controllers and processors, respectively code-owners, deliberately allowed for this degree of uncertainty. However, following the involvement of supervisory authorities and given the additional efforts these controllers and processors spent compared to others, this should be reflected by default. SCOPE Europe and SRIW acknowledge that it is hard to pre-determine the weight of such factor. Such a clarification is not required. To foster the acceptance and implementation of codes of conduct in general, it suffices to have one anchor of legal certainty that such voluntary and additional investments are worth it.

Ad 3: This scenario will likely speak for itself. Also, to protect tools such as codes of conduct and certifications, such clarification will be appreciated. Especially once understanding that codes of conduct are a new and yet largely unknown mechanism under GDPR. Any abuse and subsequent public communication thereof, is suitable to demolish any trust in the mechanism as such. Therefore, a clarification may also act as a preventive measure, thus ensuring the added value for data subjects in general.

As products of co-regulation, codes of conduct are submitted to a substantial process of scrutiny by several supervisory authorities, especially when they bear a transnational scope. In addition to the development of robust material safeguards which are subject to the approval process, codes of conduct require an **effective enforcement mechanism**. As according to Article 41 GDPR, compliance is enforced by independent monitoring bodies that not only must be accredited by the competent supervisory authority, but that are, in their turn, also subject to the scrutiny of the latter, regularly reporting its activities. Furthermore, since the monitoring body shall take appropriate action in cases of infringement of the code of conduct, a framework of ongoing due diligence is established. **Given this robust background, those instruments offer high levels of legal certainty and can positively complement the enforcement of European data protection law.**

Against this background and considering GDPR's core objective when incorporating codes of conduct – which is to support harmonized and transparent regulatory implementation – **properly clarifying mitigation effects is key**. Otherwise, the lack of clear guidance regarding the benefits of adhering to these tools can jeopardize the achievement of the abovementioned objectives.

3.2 Applicability of the Guidelines to Article 41 Accredited Monitoring Bodies

On a second dimension, the Guidelines do not make a clear statement on its applicability to private accredited monitoring bodies but does declare the established criteria applicable to "*controllers and processors according to article 4(7)(8) GDPR*". In that respect, **further guidance is welcome on how those will apply to the specificities of the functioning of a monitoring body**.

In accordance with step 2 of the Guidelines, the turnover of the undertaking is one relevant element to be taken into consideration when seeking to impose an effective, dissuasive, and proportionate fine, pursuant to Article 83(1) GDPR. However, **this point raises further questions of the extent to which turnover can be an accurate baseline for private monitoring bodies**.

Not only the turnover of a monitoring body can be difficult to determine (e.g., in the case of internal monitoring bodies), but it also depends on the number of codes of conduct being monitored, as well as on any other activities performed by the referred entity. **If the total turnover of a monitoring body was to be the basis for assessment, irrespective of the specific violation in a particular case, it would make little sense for private monitoring bodies to engage in the monitoring of more than one code of conduct.**

In this regard we must highlight that a private monitoring body that monitors several codes of conduct can set up its structures and processes way more efficiently and thus reduce the costs for adherent companies while doing so. **Such scalability allows for wide accessibility, particularly for small and**

medium-sized companies, as intended by GDPR. However, if the imposition of fines is primarily based on the general turnover of the private monitoring body, this cost reduction effect, which, in the view of SCOPE Europe and SRIW, is necessary for the establishment of the mechanism in the market, would be nullified.

Finally, such an approach also appears to jeopardize the safeguarding of the financial independence of private monitoring bodies. Therefore, given the abovementioned reasons, if a private monitoring body is entitled to concomitantly carry out different activities – as long as they do not unduly influence project-specific independences –, **the turnover reference for administrative fines should be solely connected to the relevant activities**. This segmentation can guarantee that the financial sustainability of other projects is not unduly compromised.

Key Notes

We would like to thank the EDPB for granting stakeholders the opportunity to provide their feedback on new guidance as well as for past projects. We consider the guidelines to be an essential piece of guidance, as fostering harmonization in the methodology used by supervisory authorities to calculate the number of fines is essential to ensure that key administrative and democratic principles such as predictability and legal certainty are maintained.

We greatly appreciate that the guidelines refer to the fact that adherence to codes of conduct pursuant to Article 40 of the GDPR or approved certification schemes pursuant to Article 42 may be a mitigating and relevant factor in the decision whether to impose a fine and the amount of the administrative fine, as this suggests that codes of conduct can provide legal benefits. However, we must recommend that references to the legal benefits of codes of conduct are made clearer, as well as the reason why adherence to an approved code of conduct is a positive factor.

We believe the establishment of fines shall be layered according to the following likely scenarios to emerge:

1. Shall an infringement be a result of a non-communicated new interpretation of the law by the supervisory authority, which has not been aligned with the requirements of an approved code, by default no fine shall apply.
2. Shall an infringement be a result of an unintentional/non-abusive negligence, the supervisory authority, in accordance with Article 83 (2) GDPR, shall by default consider the voluntarily adherence to an approved code of conduct as a mitigating factor.
3. Shall an infringement be a result of a gross/abusive negligence, the supervisory authority shall by default consider the voluntarily adherence to an approved code of conduct as an aggravating factor.

Finally, further guidance is welcome on the applicability of the criteria established by the Guidance in the context of accredited monitoring bodies. A direct application of the Guidelines towards monitoring bodies might negatively affect their role under GDPR, especially when it comes to having the (general) turnover as a reference point.

selbstregulierung informationswirtschaft e.V.

SCOPE EUROPE

About SRIW
Selbstregulierung Informationswirtschaft e.V. is a non-profit association supporting the self-regulation of the information economy. It acts as a think tank to discuss and debate key issues in digital policy and provides an umbrella organisation for a range of self-regulatory measures in the digital industry. We are calling for suitable regulatory methods to foster innovation and the digital transformation and, at the same time, promote corporate social responsibility, in particular with regard to the appropriate measures for data and consumer protection.

About SCOPE Europe
SCOPE Europe sprl / bvba (SCOPE Europe) is a subsidiary of SRIW. Located in Brussels, it continues and complement the portfolio of SRIW in Europe and is an accredited monitoring body under the European General Data Protection Regulation since May 2021, pursuant to Article 41 GDPR. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers and is engaged in other GDPR code of conduct initiatives.