EDPB consultation on draft Guidelines 04/2022 on the calculation of administrative fines under the GDPR

Introductory remarks: tackling fragmented GDPR interpretations as the underlying condition for harmonized enforcement

The GDPR's impact cannot be understated as its adoption was a clear global milestone for data protection and privacy rules. It not only provided upgraded rights to consumers but aimed at harmonising the rules across Europe. In this context, FEDMA welcomes the EDPB's Draft Guidelines which are expected to lead to further consistency among supervisory authorities on how GDPR fines are calculated. Nevertheless, the harmonization in the calculation of administrative fines should run in parallel to the harmonization in the interpretation of the GDPR in order to be effective. Over four years of GDPR implementation, Data Protection Authorities (DPAs) have made full use of the margin of manoeuvre available under the text.

Fragmentation is not only due to national laws, but also to national interpretation and guidance by DPAs going beyond the GDPR text. For example, this is the case concerning the use of Legitimate Interest for direct marketing purposes: in the 2019 guidelines from the Netherlands, the DPA said that legitimate interest cannot be used for processing for commercial purposes, thus clearly going against the letter and spirit of the GDPR (see Recital 47 GDPR). The persistence of diverging views and approaches feeding the fragmentation between Member States was also highlighted in the European Commission's Report on the evaluation and review of the GDPR.[1] As such, until the GDPR is interpreted differently across the Member States, the same infringement will still result in diverging fines even where the same methodology for the calculation of the fine is applied. FEDMA therefore believes that ensuring consistency in the interpretation of the GDPR is the *sine qua non* condition for its harmonized enforcement.

I. Striking the right balance between national discretion and EU-level harmonized enforcement

Though the GDPR provides that the calculation of the amount of the fine is at the discretion of each national supervisory authority, this approach has led to significant diverging practices across the Member States, undermining the harmonization of the EU data protection framework.

For example, the German, Danish and Dutch Data Protection Authorities (DPAs) have made different standard models for calculation of fines. While the German model is to rank companies by their size and turnover and then calculate a basic value which is then multiplied by a factor depending on the severity of the offense, the Danish model only defines standardised fines based on the size of companies according to their turnover, with adjustments due to the specific circumstances. The Dutch model, on the other hand, sets standard fine brackets for different categories of infringements without reference to turnover. The concept of "turnover" itself, not defined by the GDPR, has also been subject to different interpretations which, combined with varying calculation methodologies of fines, increases a fragmented GDPR enforcement.[2]

[1] Communication from the Commission to the European Parliament and the Council - two years of application of the General Data Protection Regulation, Harmonised rules but still a degree of fragmentation and diverging approaches

[2] While the Danish guidelines refer to the definition of net turnover in the Accounting Directive, Article 2 nr 1(5), i.e. 'the amounts derived from the sale of products and the provision of services after deducting sales rebates and value added tax and other

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

Such lack of consistency sets the ground for an increasingly unfair level playing field: while some European players are subject to the oversight of stricter DPAs in the Member States where they are headquartered, other non-EU companies choose to establish their EU headquarter in countries where the DPAs are known to have a more lenient approach to GDPR enforcement, including in the calculation of fines ("forum shopping").

In this context, though the EDPB's suggested harmonisation of methodology across Member States has the potential to achieve greater transparency and consistency of enforcement penalties, FEDMA believes that the Draft Guidelines still provide DPAs with significant flexibility, thus curbing legal certainty and harmonization. This is the case, for instance, of:

- The possibility for DPAs to deviate from the methodology provided by the EDPB as a whole (Paragraph 10).
- the criteria for assessing the severity of the violation where the EDPB holds that supervisory authorities "may" only weigh them in, depending on the circumstances (Chapter 4.2).
- infringements where it could be possible, at the discretion of the supervisory authorities, to impose a fine of a predetermined, fixed amount (Paragraph 18).
- the imposition of a deterrence multiplier to ensure a dissuasive fine which is left at the discretion of each DPA (Paragraph 144).

More generally, given that each DPA will have to carry out the assessment of the fine "in accordance with the specific characteristics of each case" (Article 83 GDPR), there is a great risk that each supervisory authority will implement its own methods of calculation and that divergences in interpretation will remain.

It is therefore fundamental to strike the right balance between the DPAs' independence in assessing the amount of a fine and the pressing need for harmonisation on GDPR enforcement. In this context, FEDMA calls on the EDPB to reconsider the statement whereby the Guidelines would only harmonize the starting point and methodology used to calculate a fine and would leave out the outcome (Paragraph 5).

Additionally, to balance the degree of flexibility, we stress the need to harmonize and increase the transparency about the DPAs enforcement activities and the way the EDPB's methodology will be applied. Enhanced publicity and transparency about imposed fines will strengthen their deterrent effect which will be otherwise limited since there will be no signals of the cost of non-compliance. Providing additional information on the fines can also have an educational effect and lead to changes in behaviour. We therefore regret that the Draft Guidelines emphasize that DPAs are not obliged *to provide reasoning surrounding aspects of the Guidelines that are not applicable* (Paragraph 6).

Finally, the Guidelines should also encourage national administrative courts reviewing a DPA's decision to refer to the proposed methodology when making their own assessment of the case. For instance, following the appeal by a plaintiff, the Court of The Hague lowered a fine[3] issued by the Dutch DPA in 2021 based on its own assessment on the seriousness of the infringement and on the mitigating factors. Though their assessment may differ from the DPAs, in order to avoid further fragmentation, it thus fundamental that even administrative courts take into account the same criteria as the DPAs when reviewing the imposition of a GDPR fine.

taxes directly linked to turnover', in their case against Twitter, the Irish DPA referred to the revenue stated by the firm in the annual report for the preceding year.

[3] Court of The Hague, Case AWB - 20 _ 1516, 31 March 2021

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

II. Ensuring that DPAs appropriately apply all corrective measures under the GDPR

The significant importance of the circumstances of each infringement case is repeatedly stressed throughout the Draft Guidelines. This approach encourages DPAs to carry out a case-by-case assessment where the various criteria for the calculation of the fines are taken into account to the extent that they are relevant to the specific case. In line with this approach, we believe that the Guidelines should also clarify that the imposition of an administrative fine is only one of the corrective tools available to the supervisory authorities under Art.58(2) GDPR, including warning, reprimand, order to comply to a data subject request, order to bring processing operations in compliance, order to withdraw a certification, etc.

As to avoid making the imposition of fines the *de facto* enforcement model of the GDPR, the Guidelines should thus point out that other GDPR corrective options may be much more efficient, proportionate and dissuasive in light of the specific circumstances of the case. In the same vein, we believe that the statement that the GDPR imposes a substantially increased level of fines (Paragraph 1) constitutes an overstatement. Article 83 of the GDPR only sets the upper limits of the fines that can be imposed in a given case, but does not as such increase their amount. The definition of the amount of the fine will always depend on the specific context of the infringement and be subject to the overarching principle of proportionality.

III. Adding further examples to facilitate legal certainty and consistency

FEDMA welcomes the concrete case studies provided in the Draft Guidelines to foster the explicability of specific concepts and provisions, e.g. absence of link between processing operations, plurality of actions, etc. We therefore invite the EDPB to strengthen this pragmatic approach which would also enhance legal certainty and the organisations' predictability to assess their risk for GDPR non-compliance. Specifically, FEDMA recommends providing additional examples concerning the application of:

- the principle of speciality (Paragraphs 32-25)
- the principle of consumption (Paragraph 37)
- Fixed amounts to certain types of infringements (Chapter 2.3). Though we recognize the impossibility to include an exhaustive list of circumstances where DPAs could apply a fine of a predetermined, fixed amount, a few practical examples would also contribute to foster a harmonized approach.

IV. Assessment of the seriousness of the infringement –

FEDMA welcomes the reference to the need to consider all circumstances of the case in assessing the seriousness of the infringement (Paragraphs 52 to 55). However, we would welcome more developments on the cases where the data does not enable the direct identification of the data subjects by the controller and where it is only the data subject who can recreate a link between the data and him/herself. This is the case in particular when the controller only processes pseudonymised online identifiers received from a cookie ID that can only be retrieved by the data subject. In such case, the likelihood and severity of harm for the data subject is trivial to simply inexistant as the controller is unable to identify the data subject, unless the data subject provides his/her cookie ID to exercise his/her right of access. In such instance, the level of risk remains trivial to inexistant (and should therefore by no means be considered as a serious infringement):

- even if the purpose of the processing is to monitor, evaluate personal aspects or take a decision, such as the decision to show an online advertisement (Paragraph 54(b)(i)),
- even if the scope of the processing is broad (Paragraph 54(b)(ii)), or

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

- even if the number of data subjects is high (Paragraph 54(b)(vi)).

V. Clarifying the intentional or negligent character of the infringement in specific circumstances

The Guidelines do not sufficiently embed the risk-based approach of the GDPR (performance of a DPIA, implementation of security measures, assessment of risk in the context of a data breach…). The Guidelines should clearly state that any risk assessment performed by the controller in good faith in order to assess the risk and identify the measures necessary to mitigate that risk should not lead to being considered as an intentional infringement of the GDPR. This could be the case where the DPA disagrees with the analysis of the controller and decides to fine such controller where the risk analysis has led to breaching GDPR (Paragraphs 56 and 57).

VI. Considering the application of privacy-preserving techniques on the data affected

Though the GDPR provides that certain categories of data deserve special protection due to their sensitive nature (Article 9 GDPR), we believe that the Draft Guidelines' approach whereby infringements related to special categories of data inevitably increase the seriousness of the infringement itself overlooks other relevant considerations in regard to the data affected. In line with the case-by-case assessment which the DPAs are called to apply throughout the Draft Guidelines, the analysis over the type of personal data affected should also take into account the wide range of techniques that enable to transform personal data so that it does not directly identify a data subject and the possibility or impossibility for the controller to (re)identify the data subject. FEDMA thus recommends providing that the use of privacy-preserving techniques to pseudonymize, anonymise, hash, aggregate, de-identify or re-identify the personal data affected should account at the stage of determination of the starting point for calculation of the fine and not only as a mitigating factor (Paragraphs 79 and 80).

VII. Further endorsing adherence and compliance to approved codes of conduct as mitigating factors

FEDMA welcomes the reference to adherence to approved codes of conduct among the criteria which DPAs may take into consideration when calculating a GDPR fine. Nonetheless, we believe that paragraph 104 should state more clearly that adherence to a Code of Conduct and the absence of sanction by the monitoring body should generally constitute a mitigating factor in the calculation of a fine. GDPR Codes of Conduct are not mere compliance tools as they can provide *ad-hoc* requirements and safeguards going beyond the standard obligations of the GDPR to limit the risks linked to the processing of personal data by professionals in a specific sector. Adherents to a code are also subject to regular reporting obligations towards the designated monitoring body or any other body in charge of the implementation of the code to demonstrate compliance with the provisions. As such, adherence and compliance with a Code of Conduct is not a mere commitment or formality: in order to reap the benefits of a GDPR Code, an organization must invest significant resources and implement a wide range of technical, legal and organizational measures. We therefore believe that such voluntary efforts, which exceed a baseline GDPR compliance, should be more substantially regarded as a relevant mitigating factor by supervisory authorities.

VIII. Including the organisations' balance exercise between different fundamental rights as a mitigating factor

Article 83(2)(k) of the GDPR is quite open in terms of the circumstances that may constitute a mitigating factor leading to the reduction of the amount of the fine. We would recommend including a reference to Recital (4) of the GDPR which provides that the right to the protection of personal data must be balanced against other fundamental rights. In some instances, controllers and processors are bound to balance the fundamental right to data protection and other fundamental

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

rights (freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, etc). In the absence of clear guidelines on how to balance different fundamental rights, DPAs should acknowledge the complexity for companies to balance these different rights appropriately by considering the need to comply with other fundamental rights as a mitigating factor in the calculation of a fine.

***

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org