



European Tech Alliance Response to the public consultation of the European Data Protection Board regarding Guidelines on the calculation of administrative fines under the GDPR

June 2022

“ Foreword

The European Tech Alliance (EUTA) welcomes the opportunity to provide comments to the European Data Protection Board (EDPB) Guidelines on the calculation of administrative fines under the GDPR (Guidelines 04/2022) (“the Guidelines”). We broadly support the EDPB’s objective to develop a common approach for supervisory authorities as regards calculating the amount of fines and to complement previous Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (WP253). At the same time, we believe there are certain areas which require careful consideration and that we believe are important to take into account when finalising these Guidelines. We set out below some comments in this regard.



Kristin Skogen Lund

Kristin Skogen Lund
President of the EUTA

Aurelie Caulier

Aurelie Caulier
Chair of the EUTA

I. General comments on the GDPR enforcement scheme

Article 58(2) of the GDPR provides a wide array of corrective tools to the DPAs (warning, reprimand, order to comply with a data subject request, order to bring processing operations in compliance, order to withdraw a certification...). Imposition of an administrative fine pursuant to Article 83 is only one of these tools. It is important that the Guidelines clarify this upfront so as not to make the imposition of fines the “de facto” enforcement model of the GDPR whereas other options may be much more efficient, proportionate and dissuasive in light of the specific circumstances of the case.


Similarly, the Guidelines could be interpreted to imply that administrative fines should always be imposed in case of a found infraction under the GDPR. However, national authorities may also choose to close an investigation without any sanction or issue a reprimand. EUTA would appreciate it if this could be clarified in the Guidelines. Also, EUTA would appreciate if the EDPB could provide guidance, either in the Guidelines 04/22 or separate, on when supervisory authorities may choose **not** to impose any fine when an infraction has been found.

In the same vein, the statement that the GDPR imposes a substantially increased level of fines (Paragraph 1 of the Guidelines) appears as 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.

II. Relevance in a context of significant divergences

In the first four years of the GDPR, there have been wide differences in the enforcement approaches of the DPAs. For instance, the Dutch *Autoriteit Persoonsgegevens* has had a “fining” policy since 2019, while few others have such a policy even today. Significant divergences as regards fine percentages also exist within the same authority. In Belgium, for instance, the Belgian Data Protection Authority imposed a fine of 0.0000037% of Google’s turnover in one case, a fine of 0.88% of the turnover of a small undertaking in another (its “Jubel” cookie case) and a fine of 10.15% of IAB Europe’s turnover in yet another. Similarly, the Italian Garante imposed a fine of 0.2% for telecommunications operator TIM but 5% for its competitor Vodafone Italia, despite both cases involving infringements of the same articles of the General Data Protection Regulation (GDPR). Similarly, there is a wide divergence of approach in the calculation of fines between the [Irish DPC and the German DPA in Decision 01/20 - Twitter International Company.](#)

While each case does indeed merit its own



specific assessment, the broad range of percentages applied indicates that there are significant divergences in the existing practices of supervisory authorities - divergences which would have to be bridged overnight if the “starting point” tiers of Guidelines were to become applicable. In our view, the application of “starting amount” tiers, as included in the draft Guidelines, could have the perverse effects of a consistent approach.

On the one hand, it could lead to a disregard for the Guidelines by certain supervisory authorities that may continue their current practices, thereby not addressing the primary objective of the Guidelines. Such lack of consistency has the unfortunate effect of recreating the fragmentation on the EU market that the GDPR was intended to address in the first place when it replaced Directive 95/46.

On the other hand, it could lead to a significantly different fining approach post-guidelines compared to previously. In the latter case, it could be argued that this results in an unjustified discrimination between two controllers purely on the basis of when the supervisory authority imposed its fine – before or after finalisation of the guidelines – as the controller fined before finalisation of such Guidelines may be subject to a far more favourable fining approach than the one fined afterwards. Given that the EDPB’s guidelines are not binding, there will be no actual and objective justification for such discrimination.

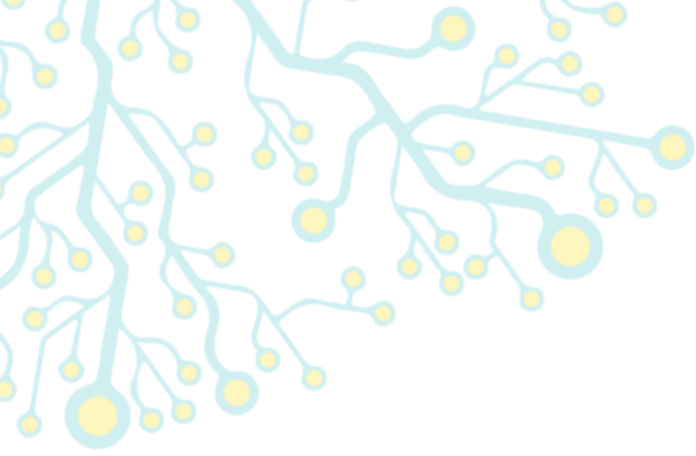
More importantly, the lack of coherent approach in the calculation of fines has the

effect of distorting the market conditions in different member states and leads to creating an unfair level playing field on the EU market. This leads to a disadvantage for some European players whose headquarters subject them to the oversight of a stricter DPA. It also creates an unfair treatment with non-EU companies which tend to establish their EU headquarters in countries where the DPAs are known to have a more lenient approach to GDPR enforcement, including in the calculation of fines (“forum shopping”). It is therefore of the utmost importance that the Guidelines find the right balance between the DPAs’ independence in assessing the amount of a fine and the pressing need for harmonisation on GDPR enforcement.

We therefore recommend removing the sections relating to the starting points and tiers from the Guidelines. Alternatively, instead of starting points and tiers at this stage, and in order to make a transition towards a new, consistent approach smoother and more legally sound, we recommend that the EDPB starts to compile its own database of fines, in which various relevant factors could be listed in order to facilitate a classification in the future.

III. Outside observer

In paragraph 28 and example 1a, reference is made to an “outside observer” as the standard by which to judge whether specific processing operations form one coherent conduct. However, the Guidelines do not specify which level of awareness is attributed to the “outside observer”.



In this respect, EUTA recommends that the EDPB add that the outside observer is presumed to be the average data subject. This approach would enable controllers to approach any processing operation from the perspective of their intended audience (which they are in any event supposed to take into account when e.g. determining which type of language to use in a privacy statement or notice, etc.).

IV. Guiding principles (specialty, subsidiarity and consumption)

The Guidelines contain in paragraphs 30 and following reference three key principles regarding concurrence, namely specialty, subsidiarity and consumption. These principles are provided in an abstract manner, without examples that would make them more tangible.

For instance, paragraphs 32-35 include various references to the principle of specialty and case C-10/18 P before the Court of Justice of the European Union (*Marine Harvest*). It appears that the EDPB considers that where a provision of the GDPR is a concretisation of one of the data protection principles set out in Article 5 GDPR, an infringement of the more specific provision “supersedes” the infringement of Article 5 GDPR.

While EUTA applauds this perspective, the lack of examples makes this difficult to assess. In fact, many supervisory authorities today issue rulings which identify violations of both the principle and the specific provision (for instance, many findings of a violation of Art. 32 GDPR are considered by supervisory authorities to also be a violation of Art. 5(1)(f) GDPR). We therefore believe that some examples of violations of Art. 5 GDPR (the data protection principles) that are not violations of other provisions of the GDPR may be helpful. Otherwise, there is a risk of the Guidelines being challenged e.g. by activists in terms of their compatibility with the very text of Article 83(4) and (5) GDPR, which provide for higher maximum fines for violations of e.g. Article 5 GDPR (Article 83(5) GDPR) than for violations of Articles 25 to 39 GDPR (Article 83(4) GDPR).

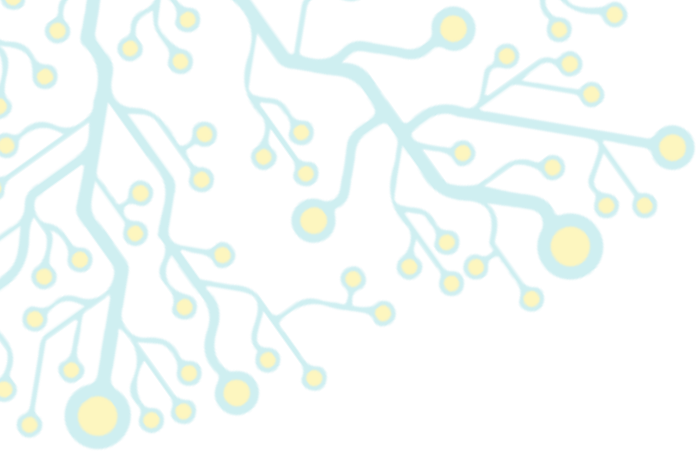
V. Unity of action

Section 3.1.2 of the Guidelines examines the question of unity of action, and notably the example where “[a] controller sends bundles of marketing emails to groups of data subjects in different waves during the course of one day without having a legal ground”.

In our view, already from a functional perspective, there should be no reason to consider the sending of the various waves of emails as separate processing activities. The sending of marketing emails to groups in different waves is determined by technical restrictions. Most email service providers impose limits on the number of recipients for one email, often in part for service quality reasons and in part in the context of the fight against spam and abuse of email services.

Perhaps a better alternative example might be the case where such waves are sent “during the course of one week”, as in such a case the controller chooses to spread them out, but in practice they remain related and part of the same coherent whole.





VI. Seriousness and Gravity of infringement

We welcome the reference to the need to consider all circumstances of the case in assessing the seriousness of the infringement (Paragraphs 52 to 55 of the Guidelines). We would welcome more elaboration on the cases where the data does not enable the direct identification of individuals by the controller, or the processor in case of analysing specifically a processor scope, 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 a case, the likelihood and severity of harm for the individual is trivial to simply nonexistent as the controller is unable to identify the data subject, unless the data subject exercises provides his/her cookie ID to exercise his/her right of access. In such instance, the level of risk remains trivial to nonexistent, and should therefore by no means be considered as a serious infringement:

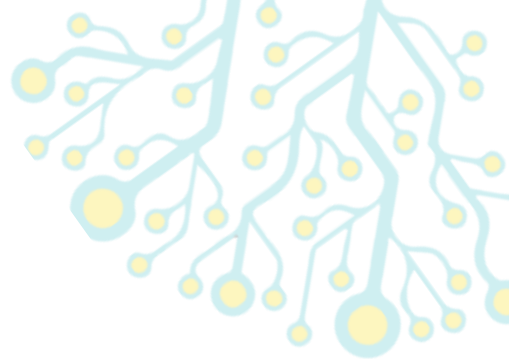
- even if the purpose of the processing is to monitor, evaluate personal aspects or take a decision - such as the decision to show an online advertisement (Paragraph 54(b)(i) of the Guidelines),
- even if the scope of the processing is broad (Paragraph 54(b)(ii) of the Guidelines), or
- even if the number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

In this light, we propose that the Guidelines 04/2022 consider explicitly, as an example, that international data transfers outside the European Economic Area, of non-directly linkable online identifiers (such as a first-party cookie) or any other pseudonymised identifier (based on the standard data protection clauses adopted by the Commission or any other appropriate safeguard covered in Article 46 GDPR) should be considered as pseudonymised data, and shouldn't be considered as a serious infringement. For such interpretation to be valid, such identifiers cannot be directly linked to an individual by the company processing the data outside the EEA or any other party that could access such non-directly linkable identifiers from outside the EEA.

In the section on the gravity of the infringement (section 4.2.1(b)), there is a reference to the fact that “[w]hen the nature of processing entails higher risks [...] the supervisory authority may consider to attribute more weight to this factor”. Examples of “higher risk” processing are also included: “e.g. where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for the data subjects, depending on the context of the processing and the role of the controller or processor”.

The notion of “high risk” processing is linked to Art. 35 GDPR and the notion of the data protection impact assessment (DPIA). Yet, other guidelines of the Article 29 Working Party (and endorsed by the EDPB) and of national authorities (e.g. the CNIL) already





set out examples of “high risk” processing activities and how to identify or assess them. In this context, the reference in the Guidelines to processing activities whose “purpose is to monitor, evaluate personal aspects” could be viewed as expanding the scenarios for which a DPIA is required.

For that reason, we recommend deleting the words “to monitor, evaluate personal aspects” to avoid any confusion.

VII. Starting point calculation

EUTA would appreciate more details in the examples in paragraph 63 as well as less broad ranges for the suggested starting amounts for further calculation in order to avoid discretionary assessments. In one of the provided examples, the starting amount for further calculation is suggested to be at a point between 20 and 100 % of the legal maximum included in Article 83(5) GDPR, which is a too broad range to give any clear guidance.

Further, the EDPB’s suggested method for calculating a starting point for a fine does not always seem consistent.

For instance, in paragraph 67, which refers to three thresholds (“*an undertaking with an annual turnover not exceeding 100 million euros, an annual turnover not exceeding 250 million euros and an annual turnover not exceeding 500 million euros*”), there is the suggestion that the starting point could be “50% of the identified starting amount” for “*undertakings with an annual turnover of €250m or above*”. In other words, the “50% of the starting amount” idea could be read as being only for undertakings with a turnover between 250 million euros and 500 million euros.

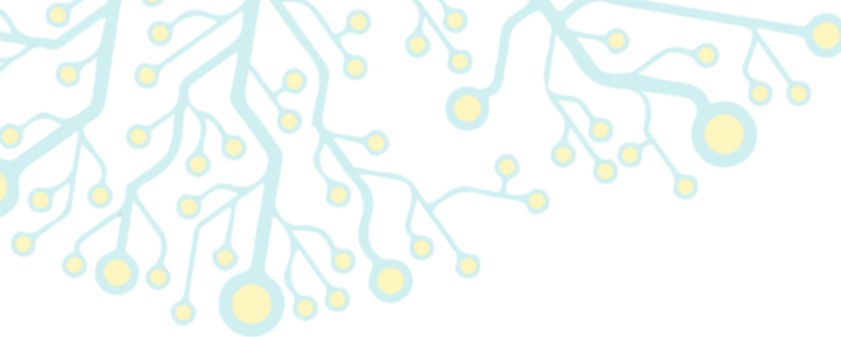
Example 6a, which follows, applies the “50% of the starting amount” idea to an undertaking with a significantly higher annual turnover, which makes it difficult to

understand what the EDPB’s suggestion actually is: “*Based on the turnover of the undertaking (€8 billion), the supervisory authority may consider to further reduce this amount to 50% of the identified starting amount corresponding to the seriousness of the infringement.*”

While this outcome – a lower fine – is ultimately more favourable to the undertaking in question, we strongly favour certainty and clarity in the suggested method. We therefore believe that the methodology should be further clarified and inconsistencies are addressed in the final Guidelines.

VIII. Intentional or negligent character of the infringement

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 a controller where the risk analysis has led to breaching GDPR (Paragraphs 56 and 57 of the Guidelines).

IX. Categories of personal data affected

Paragraphs 58 and 59 of the Guidelines only consider the cases where special categories of data and regular categories of data are processed to quantify the seriousness of the infringement in each individual case. This binary approach does not take into consideration the wide range of techniques that enable to transform data so that it does not directly identify an individual and the possibility or impossibility for the controller to identify the individual. Considerations on whether the data was pseudonymized, anonymised, hashed, aggregated, de-identified or re-identifiable should also be taken into consideration at the stage of determination of the starting point for calculation of the fine and not only as a mitigating factor (See Paragraphs 79 and 80 of the Guidelines).

X. Adherence to approved codes of conduct

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. Adherence and continued compliance with a code of conduct that may go beyond the standard obligations of the GDPR requires substantial investment from companies that should be rewarded for their voluntary efforts.

XI. Mitigating factors

In paragraph 77, the Guidelines suggest that *“measures spontaneously implemented prior to the commencement of the supervisory authority’s investigation becoming known to the controller or processor are more likely to be considered a mitigating factor, than measures that have been implemented after that moment”*.

This position appears to ignore the fact that in some cases, a supervisory authority may have a novel interpretation of specific concepts of the GDPR or may apply the GDPR to industry- or sector-wide practices that have not been questioned since before the GDPR was adopted. Similarly, there are cases where a supervisory authority has not yet adopted any guidance on a particular issue and has not indicated that in its view there may be issues in relation to certain practices. In such a context, measures implemented rapidly after the controller or processor becomes aware of the new guidance or investigation should also be taken into consideration.

In addition, there are situations where data subjects file complaints with supervisory authorities without even informing controllers of the existence of an issue in their opinion. In such a case, measures taken rapidly after they are informed of the existence of such an issue should also be taken into account.

Finally, 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 adding 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 rights (freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business...). Pending the setting up of a formal regulatory cooperation to address this situation, DPAs should have the possibility to 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.

EUTA therefore recommends adding a level of nuance to the statement in paragraph 77 of the Guidelines.

XII. Dissuasiveness

EUTA suggests that the Guidelines takes into account that the dissuasiveness should not only be assessed from a direct economic perspective, i.e. the size of any administrative fines, but also from an indirect perspective. For example, the fact that a decision may lead to bad press, lack of customer trust, and affect the stock price, may be sufficiently dissuasive for many companies.



Final Say

We thank you for considering these points and remain at your disposal for any clarification you may require.

