Spolek pro ochranu osobních údajů

**Comments on the EDPB's draft "Guidelines 4/2022 on the calculation of administrative fines under the GDPR"**

We welcome the opportunity to present our comments to the recently published EDPB draft Guidelines 04/2022 on administrative fines (Guidelines).

**General comments**

We appreciate the effort of the EDPB to provide more harmonisation and predictability to the process of fine calculation, moreover, we understand the topic to be rather complex, involving numerous criteria to be considered.

Unfortunately, we are in many ways disappointed by the approach applied by the Guidelines and beside a number of valuable pieces of advice on how to possibly approach fine calculation of the fine under the GDPR provided, in some respects we believe the Guidelines bring about number of issues we find rather controversial, in particular the Guidelines:

a) may in fact discourage the willingness of controllers and processors to comply with their obligations arising from the GDPR and thus, inter alia, contribute to the weakening of the position of data protection officers,

b) may possibly contribute to a discriminatory approach in the process of fines calculation,

c) in some parts are inconsistent with the GDPR provisions.

We believe that such a fundamental issue as the administrative fines calculation in enforcing the GDPR would have deserved a more detailed expert discussion before the draft Guidelines were published for consultation. This is all the more significant given that in some countries (eg Germany) similar initiatives ("fine tariffs") have already been set up by national supervisory authorities and have met with contradictory acceptance.

Out of the key questions we have identified in the Guidelines, we would like to draw your attention specifically to the following points:

1. In our view, the Guidelines are not built around the two main pillars of the GDPR: **(i) the protection of individuals against the unauthorised processing of their personal data; (ii) risk-based approach**. It seems like certain provisions of the Guidelines could have been driven by the only goal being to fine controllers or processors instead. It seems as if imposing fines was the main purpose of the GDPR and the only enforcement tool provided to the supervisory authorities without primarily considering the impact of the non-compliance into the rights and freedoms of individuals.

2. The Guidelines do not sufficiently address the possibility of using other corrective powers provided to the supervisory authorities and their relationship to fines in order to create an



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

efficient framework for GDPR enforcement. At the same time, from the point of view of the protection of the rights of individual data subjects, the application of other corrective powers can in many cases be a far more effective measure than solely imposing a fine.

3. The principle of the ultima ratio of criminal and administrative repression (see also the previous point) as one of the main principles of European public law is unfortunately not emphasised by the Guidelines.

4. We miss the legal basis of the "minimum amount of fine" concept newly introduced by the Guidelines where the minimum level of fine is derived primarily from the turnover (see also the proposals of the German Datenschutzkonferenz) of the breaching organisation. We consider such an approach lacking a legal basis in the GDPR to be rather controversial.

5. In our view, the Guidelines misinterpret the limitation on fines under Article 83 (4) and (5) of the GDPR not as the highest possible amount of the fine (upper limit), but as the upper limit of the usual interval in which the fine is to be imposed.

6. The Guidelines misinterpret the GDPR with regard to the basis for calculating the fine for a group of undertakings. This interpretation contradicts some language versions of the GDPR and is therefore, in our view, incorrect and misleading.

7. In some circumstances, the Guidelines incorrectly allow only 'neutral' and 'aggravating' circumstances to be reflected in the process of fine calculation and completely ignore any mitigating circumstances.

**Failure to take into account the main objective of the GDPR**

Article 1 (1) and (2) of the GDPR declares its objective. The second paragraph states in particular: "*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*." We believe that this is a fundamental aspect that should be the starting point for the application of the GDPR, including the assessment of GDPR violations and the imposition of administrative sanctions. Therefore, the Guidelines should also build upon this objective. The aim of imposing fines and GDPR enforcement in general should not be primarily to increase the revenue of the state budget or to punish a commercially successful company for being successful (although we recognise the need (see Article 83 (1)) to impose effective and dissuasive fines). From that point of view, it is unfortunate, that the Guidelines, taking into account the „*gravity of the infringement"* in paragraph 54, state *„The level of damage suffered and the extent to which conduct may affect individual rights and freedoms"* only in the last place. It is also not clear to us why the context should be taken into account when setting the amount of the fine, as suggested by EDPB in paragraph 54 (a)(i): "*including the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc)*". It appears that the EDPB intends to set the amount of the fine here only on the basis of the nature of the activity in which the GDPR was infringed. Although such a distinction may play a role in some cases, the main consideration in this respect will be the ***purpose of the processing*** (mentioned under point (iii)) and, where appropriate, whether or not the activity was carried out to gain unjustified profit to the detriment of data subjects. The very nature of the activity in question (eg „business activity", „non-profit", „political party", etc.) should not, in our view, play a significant role. It is not clear, for example, why unauthorised processing should be evaluated more strictly (or otherwise), e.g. in the context of processing health data for research purpose carried out by entrepreneurs or non-



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

profit organisations. In our opinion, the overall impact on the rights of data subjects will be more important. This distinction is also not supported by and goes beyond the text of GDPR.

In this connection we miss the need to apply a risk-based approach to the fine calculation related to the individual's rights and freedoms. The implications caused by non-compliance in the area of data subjects´ rights and freedoms will not in most cases depend on the "nature" of the organisation but on the result of its non-compliance.

Similarly, we do not consider it ideal to emphasise local, national or cross-border processing with the suffix: "*This element highlights a real risk factor, linked to the greater difficulty for the data subject and the supervisory authority to curb unlawful conduct as the scope of the processing increases.*" We believe that the mere fact that processing is carried out "cross-border" may not yet have any significant impact on the risk associated with processing and rather other issues are key elements, such as the impact on the data subject's rights, the type of breach, the intention or negligence, etc. On the contrary, the GDPR supports the free movement of data within the EU, as an integral part and condition of the free movement of goods, services and capital, so the indication of making cross-border processing an aggravating circumstance is contrary to both the GDPR and the basic principle of the European Union. More important aspect to consider may be for example the number of data subjects affected (see paragraph 54(a)(iv)). Finally, the implication that the reason for the stricter approach to cross-border processing is the difficulty on the part of supervisory authorities in investigating and sanctioning misconduct in such processing is also very unfortunate. The GDPR contains a set of mechanisms designed to promote and unify cooperation between supervisory authorities across the European Union.

We consider also the idea "*The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances*", far too simplistic. Although we understand the reasoning that caused EDPB to make such a comment, we must point out that many GDPR breaches (especially less serious breaches) will usually not be more serious simply because they present the core activity of the controller or processor (and vice versa, even a violation of the rights of the subjects, which is - in terms of core activities – completely marginal for the controller or processor, may be much more significant in its impact on their personal sphere). Again, we see the risk-based approach missing.

**Use of other corrective powers and "interface" between the application of fines and other remedies**

Art. 58 allows data protection authorities to order a number of remedies to the controller. We believe that the Guidelines should take into account that fines are by no means the only or legally preferred corrective powers and should also assess the possibilities of using other remedies under the GDPR. From the point of view of data subjects, it is essential that their rights are not infringed, and other remedies under Article 58 may contribute to this much more directly than the imposition of fines.

**Insufficient emphasis on the principle of ultima ratio of criminal and administrative repression**

Also linked to the above is the question whether the EDPB's unmissable emphasis on sanctions in the form of fines in the guidelines (as well as in the publication of information on its website) is entirely appropriate for effectively enforcing such a complex matter as GDPR



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

and whether it complies with the principles of European public law (the principle of the ultima ratio of administrative sanctions). We would like the EDPB to focus also on examples of good practice and to promote those controllers and processors who, in its view, show the way in which GDPR should be applied.

**Minimum amount of fines and amount of fines derived primarily from turnover**

We believe that GDPR does not set out the concept of "minimum amount of fine", nor explicitly orders that the turnover of the controller and processor concerned be (always) taken into account. If the lawmakers were interested in setting a minimum amount of fines for a tort, below which it would not be possible to impose a fine, they would certainly do so in the text of GDPR or expressively empower the data protection authorities to take it into account. At the same time, we do not consider it appropriate for a number of cases to set or derive fines from turnover (see, for example, paragraph 68). A number of situations can be imagined where such a method of setting fines will fail. E.g. ancillary service with a low turnover and number of users set up by a large entity operating primarily in other markets. It is not clear to us why such a controller or processor should be fined differently from a controller operating a fully comparable service but not achieving further turnover in other activities. We do not consider the references to the Commission's practice in the field of fines for infringements of competition rules to be appropriate, as this is a different issue with other protected interests.

If the EDPB proceeds from the assumption of the „*starting point*" principle (see the wording of paragraph 47, „*The EDPB considers that the calculation of administrative fines should commence from a harmonised starting point*"), it is not at all clear from the draft guidelines what considerations led the EDPB to such a conclusion and what is considering by EDPB as legal basis for this, especially in situations where there is an almost unlimited range of possible GDPR breaches of varying severity, impact and based on different causes.

We also do not consider the statement made in point 18 of the draft Guidelines on the possibility of imposing flat-rate fines („*In certain circumstances the supervisory authority may consider that certain infringements can be punished with a fine of a predetermined, fixed amount*.") to be fully correct and in our view it could be contrary to the requirements of the GDPR set out in Article 83 (2) (ie the requirements to take into account the circumstances of each individual case).

**Interpretation of fines under Article 83**

We consider that the amount of fines under the Article 83, ie up to a maximum of EUR 20,000,000, or in the case of an undertaking, up to 4% of the total annual worldwide turnover for the preceding financial year, does not primarily serve as a benchmark for determining the amount of the fine in the range of EUR 0-20 million (or even in another interval with a minimum amount, as proposed by the EDPB in paragraph 61), but it is indeed a matter of setting an upper „ceiling" for fines in each individual case, if imposed. In other words - it cannot be assumed for every imaginable breach of the GDPR, that a similar „type-matching" breach could be found which (in its scope or other circumstances) would justify the imposition of a fine in the maximum amount. At the same time, setting a threshold of fines as a percentage of the maximum amount (determined from total turnover) can lead to significant injustices. A completely identical breach of the GDPR **with completely identical consequences for data subjects** could lead to a very different amount of the fine for the controllers with a higher overall turnover. This might create room for an unjustified disproportion in the imposition of fines.



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

**Basis for calculating the fine for a group of undertakings**

We are familiar with the English and some other language versions of the GDPR. Nevertheless, it must be noted that it is not possible to find a provision in the Czech language version of the GDPR that would justify EDPB's view expressed in point 6.2.1, ie that the turnover of the group of companies, not the controller/processor concerned, should be taken into account when calculating fines. In the Czech language version, Article 83 (5) of the GDPR (and similarly in next paragraph 6) explicitly states: "*Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 20 000 000 EUR, nebo **jedná-li se o podnik**, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší...*". Article 4 (18) then defines an enterprise as follows: *„„podnikem" jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost* ". The enterprise is thus defined on the basis of its identity as (one) legal or natural person. The Czech language version (apart from the non-binding text of rec. 150) then leaves no room for interpretation of the calculation of the amount of fines in the sense of the approach used in competition law. It will be up to the Court of Justice of the EU to determine the correct interpretation of this part of GDPR. However, given that this is an issue of administrative punishment, the use of the principle *in dubio pro mitius* can only be recommended.

**Allowing only "neutral" and "aggravating" circumstances**

The Guidelines in many places only allow "neutral" or "aggravating" circumstances to be considered in the process of the fine setting, and any mitigating circumstances are omitted. We find such approach unfair and unjust.

First of all, such an approach does not correspond to the text of the GDPR. The GDPR itself (Article 83) assumes that administrative fines are imposed **according to the circumstances of each individual case**. In deciding whether to impose an administrative fine and in deciding the amount of an administrative fine in individual cases, due account shall also be taken, inter alia, of the steps taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83 (2) (c)), the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement (Article 83 (2) (f)), the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement (Article 83 (2) (h)) and any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement (Article 83 paragraph 2 (k)). For example, if the data breach notification is taken into account (see, for example, point 98 of the draft Guidelines), circumstances may arise which will allow a specific action made by the controller to be considered an mitigating circumstance. It can be, for example, above-standard cooperation with the supervisory authority, etc.

Another negative aspect of the EDPB's approach in this context is that it will surely demotivate the efforts of controllers and processors to take any above-standard steps when reporting a data breach or other finding of non-compliance with the GDPR. As an organisation of data protection officers, we see this as a significant risk to their work, as this approach can lead to controllers or processors losing any interest in cooperating with supervisors in addressing personal data breaches and not following advices of their DPO aiming at faster and more effective remedy of a breach of GDPR, because any above-standard efforts will not bring them any significant advantage. As with any human activity, positive motivation is also important



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

here (especially when, in the given case, it fully corresponds to the text and meaning of the GDPR and obviously also to the intention of the EU legislator).

A typical example of such an incorrect approach is the consideration in paragraph 82: "*Given the increased level of accountability under the GDPR in comparison with Directive 95/46/EC,32 it is likely that the degree 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.*" Here, we believe, the EDPB relies on an incorrect consideration of a higher degree of accountability as a factor which precludes mitigating circumstances. However, this factor "only" sets a different "level" of default measures required from the controller or processor but does not affect the fact that the circumstances of the case could be considered aggravating or mitigating depending on the context. In other words, the principle of accountability "raises the bar" for the measures applied by the controller but does not affect whether there were (and should be considered) aggravating or mitigating circumstances in a particular case or not.

Similarly, in paragraph 57, there is a consideration relating to *„The intentional or negligent character of the infringement ..."*. It is not clear for us why, on the one hand, EDPB allows the degree of culpability to be determined, but, on the other hand, it considers the form of culpability to be only at the best the neutral factor.

We also consider the view presented in paragraph 94 as not fully appropriate: *„...The absence of any previous infringements, however, cannot be considered a mitigating factor, as compliance with the GDPR is the norm. If there are no previous infringements, this factor can be regarded as neutral*." The absence of a previous breach of the GDPR can be - depending on the context - a typical mitigating circumstance (and thus in number of the member states, the competent supervisory authority is obliged to take it into account by law or applicable principles of administrative sanctioning). In our view, such an approach cannot be justified even by the wording of Article 83(2)(a)(e) GDPR, because this is to be considered only as an example.

Similarly, we would recommend not imposing additional conditions for the possibility to consider certain circumstances as mitigating (contrary to the text of the GDPR). For example, point 97 of the draft guidelines states that „*However, where cooperation with the supervisory authority* ***has had the effect of limiting or avoiding negative consequences for the rights of the individuals that might otherwise have occurred****, the supervisory authority may consider this a mitigating factor in the sense of Article 83(2)(f) GDPR, thereby decreasing the amount of the fine*." However, the GDPR in Article 83 (2) Lit. (f) takes into account rather the fact that the controller or processor acted with **the intention (purpose) of repairing or minimising the damage** rather than strictly requiring the result to be met: *("f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement"*).

Additionally, these obligations (and, for example, considerations regarding the consequences of the mandatory notification of a data breach within the meaning of Article 33 of the GDPR, see paragraph 98 of the guidelines) need to be carefully balanced with the existence and impact of the privilege against self-incrimination. Although the privilege against self-incrimination does not in itself preclude the existence of rules and obligations of controllers in Article 33 of the GDPR, it may play a role in assessing how to interpret the behaviour of controller (and in assessing its behaviour as an aggravating, neutral or mitigating circumstance).



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

**We are grateful for the opportunity to provide our comments on the draft Guidelines. However, we believe there is considerable room for review of the suggested approach towards the fines setting process for the benefit of the data subjects and motivation of responsible behaviour of the organisations.**

Prague, 27.6.2022

**JUDr. Vladan Rámiš, Ph.D.**
**Alice Selby, LLM, Ph.D., CIPP/E, CIPM**
**Mgr. František Nonnemann**
Members of the Committee
**Spolek pro ochranu osobních údajů**



Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562