noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

noyb's comments on the Draft Guidelines 4/2022 on the calculation of administrative fines under the GDPR- Version 1.0

noyb welcomes the possibility given by the EDPB to provide comments on the Draft Guidelines of the EDPB ("the Guidelines") on the calculation of administrative fines under the GDPR. We hope the following comments are useful for the EDPB:

I. General comments on the need for guidelines and the precise foreseeability of the fines

As a general comment, *noyb* considers the Guidelines as a useful document for Supervisory Authorities ("SAs") to calculate the amount of fines.

However, in the field of competition law, whereas Articles 101 and 102 TFEU did not mention any criteria for the calculation of fines, Regulation n°1/2003 only refers to two criteria in Article 23: the duration and the gravity of infringements. The first guidelines regarding fines were adopted by the Commission in 1989. That means that the Commission was able to impose fines for more than 20 years without adopting further guidelines on the matter.

The situation is quite different regarding the GDPR since Article 83(2) refers to a long list of criteria to be taken into account to determine the amount of the fine. Considering the above, and seeing that the fines under the GDPR are still relatively new, we are not sure that such guidelines should be adopted as such an early stage, with the potential effect to set in stone the calculation of fines for the future. These Guidelines would then be raised by controllers and processors to force the SAs to follow a method that might be too rigid for SAs to adopt and that might not serve the purpose of data protection law enforcement.[1]

Moreover, not only do we not see in the case-law cited by the EDPB any reference to an obligation to have guidance, but we also do not find that a requirement that such a guidance should be "*as specific as to allow a controller or processor to make precise mathematical calculation of the fine*".[2]

[1] Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, *Dansk Rørindustri A/S*, § 213.
[2] See § 60 of the Guidelines.

On the contrary, in the field of competition law, the Court already confirmed that "*the Commission enjoys a broad discretion as regards the method for calculating fines. That method, set out in the 2006 Guidelines, displays flexibility in a number of ways, enabling the Commission to exercise its discretion in accordance with Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 [EC] and 82 [EC]*"[3] – a case that seems to be in line with most national legal traditions and the EDPB may want to refer to as well.

In addition, the Court also confirmed that the Commission could "*raise the limits indicated in Regulation n°17 if that is necessary to ensure the implementation of Community competition policy. On the contrary, the proper application of the Community competition rules requires that the Commission may at any time adjust the level of fines to the needs of that policy*".[4]

The SAs should bear in mind that the purpose of the GDPR is the protection of a fundamental right, and the calculation of fines (but also the enforcement of the GDPR more generally) cannot be based on the competition law experience, as the objectives, the means, the enforcement body, and the interests at stake are different.

The SAs should keep discretionary powers to decide upon the right amount of fines to make sure that the GDPR will be effectively enforced, with fines that are deterrent, both in cross-border cases and in national cases.

We therefore welcome that the EDPB confirms its statement that *"notwithstanding cooperation and consistency duties, the calculation of the amount of the fine is at the discretion of the supervisory authority"*. We also welcome the confirmation by the EDPB that the Guidelines are only indicative, should not be misunderstood as a form of automatic and arithmetical calculation, and will be reviewed periodically by the EDPB to ensure that the level of the fines under the GDPR always remain "effective, proportionate and dissuasive".[5]

II. Dynamics of appeals

[3] See Case T-91/02n *Innolux Corp v. Commission,* § 88.
[4] Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, *Dansk Rørindustri A/S*, § 88. According to the Court, *"it follows from that case-law of the European Court of Human Rights that the scope of the notion of foreseeability depends to a considerable degree on the content of the text in issue, the field it is designed to cover and the number and status of those to whom it is addressed. A law may still satisfy the requirement of foreseeability even if the person concerned has to take appropriate legal advice to assess, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. This is particularly true in relation to persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation. They can on this account be expected to take special care in assessing the risks that such an activity entails (see Cantoni v France, cited above, § 35).*" (see § 219).
[5] See Chapter 8 of the Guidelines.

We are concerned that the level of harmonisation of the fines may become dead letter in many cases, since complainant may only have the right to appeal a decision of an SA that rejects the whole or part of their complaint and cannot challenge the level of the fine.

It is usually the controller or the processor that will challenge the level of the fine in court. Low fines will not be challenged. This will mean that details of the Guidelines will primarily be used in any challenge to a possible fine. We would therefore stress the EDPB to review each element of the Guidelines from the perspective of a controller or processor that wishes to challenge any decision by the SAs.

III. Harmonization

Moreover, it seems that, in cross-border cases, the EDPB will only be able to review the level of the fines when the case reaches the consistency mechanism.

Furthermore, the objective of harmonisation pursued by the Guidelines might not be successful in countries where the SAs do not have fining powers, such as Estonia and Denmark. In such countries where the courts have to intervene, but also in cases of appeal against the decisions of other SAs, the courts might ignore the Guidelines, considering that they are not bound by them.

That being said, we understand that the CJEU would rather follow the Guidelines of the EDPB when assessing the level of fines as reviewed by the EDPB in the context of decisions under Article 65(1)(a) GDPR. National courts should be encouraged to follow the same path to ensure a consistent approach regarding the imposition of fines under the GDPR.

IV. Concurrent infringements

The EDPB document differentiates between the situations of concurrence of offences, unity of action, and plurality of actions. It considers that different rules apply in these different situations and takes into account Article 83(3) GDPR and general principles of administrative and criminal law. In this regard, the Guidelines consider that the notion of "one sanctionable conduct" should refer to the "same or linked processing operations", as referred to in Article 83(3) GDPR.

We understand from the EDPB Guidelines that in the case of linked processing activities, either one infringement would be upheld in relation to one conduct or, in case of unity of action and several infringements, only the highest fine would be imposed (as referred to in Article 83(3) GDPR). That means that, should the SA find several violations of the GDPR (according to Section 3.2 of the Guidelines) in relation to several linked processing operations, only the highest fine would be imposed.

We support the statement of the EDPB according to which "*a sufficient link should not be assumed easily, in order for the supervisory authority to avoid infringement of the principles of deterrence and effective enforcement of European law*".[6]

Any other conclusion would lead to a limitation of the fine that an SA could impose on certain providers that perform numerous processing operations, versus other providers performing separate processing operations not obviously linked to each other would be subject to different fines since Article 83(3) GDPR would not apply.

Interaction with Article 50 CFR

We would like to highlight that the definition of a violation is interacting with the issues of multiple penalties (e.g. in case of continuous violations) and EU as well as national law on double jeopardy. If the EDPB Guidelines would therefore take the view that a vast and broad set of violations are in fact one single violation, a controller or processor may choose to continue the violations, as the first penalty would make the controller or processor immune from further fines. We are concerned that this could amount to something like a "GDPR violation tax" in certain cases. As this is a European principle, even a small fine in one Member State could block further enforcement actions by other SAs.

The scope of a "processing operation"

Unfortunately, the underlying criteria mentioned by the EDPB[7] seem to constitute an extensive interpretation of "*linked processing operations*".

For example, example 1b refers to various violations of the GDPR (lack of information provided to the data subjects, no answer to access requests, no record of processing) that are considered as "linked". We are not sure if this is a correct assessment:

- Not answering an access request (or not complying with any other data subject right) is clearly a different willful act than unlawfully processing data in the first place.
- Not responding to an access request, not complying with an objection or not processing the withdrawal of consent is clearly a distinct and separate unlawful *failure* to perform a processing operation that should not be conflated with the initial illegally illegal processing operation that generated personal data.

We are concerned that in some sectors where several processing activities could be considered as linked, this would lead to a limitation of the fine and to a clear incentive to rather engage in total non-compliance, instead of at least complying with some parts of the GDPR. This would be in tension with the EU law principles of fairness, efficiency and non-discrimination between controllers.

For example, a whole range of processing activities could be considered as linked in the context of social media platforms. They can cover the collection of data, transfers, delivering of advertising, profiling, and the exercise of all data subject rights under the GDPR. They could potentially be considered as "*contextually, spatially and temporarily*

[6] See §28 of the Guidelines.
[7] See §28 of the Guidelines.

related", and therefore considered as being linked and forming the same conduct. This link can even be artificially created by the platform.

We therefore suggest to at least remove the non-compliance with specific and separate requests for processing operations by the data subject from the examples.

Temporal connection

In addition, we are concerned that the examples of the EDPB read as giving a lot of weight towards a temporal element, as examples highlight that acts are taken place same day alike. There is no basis for a temporal element in the GDPR.

Focus on decisions and acts

We would very much propose to focus on separate acts and intentions of controllers, processors and relevant decision makers. Usually there is separate decision to have a certain processing operation, a separate decision not to update a privacy policy and not to comply with a right to objection. Consequently, Article 83(3) GDPR also refers to "intentional or negligent" infringements.

Review of national criminal law

We would suggest that the EDPB takes a closer look at existing theories under national criminal law that have to deal with similar issues. Equally, we wonder if there is relevant CJEU case law on this matter.

In addition, regarding the concurrence of offences (Section 3.1.2 of the Guidelines), the EDPB could provide some examples of cases where the principle of subsidiarity or consumption may play a role in calculating the fine when the same conduct leads to several violations.

V. Starting point for calculation

As a general comment, we share the view of the EDPS that *"identification of harmonised starting points in these Guidelines does not and should not preclude supervisory authorities from assessing each case on its merits".*[8]

Nature of the infringement

Regarding the nature of the infringement, we consider that the impact of the violation on the rights of the data subjects and their capacity to exercise such rights, but also on the ability of the SAs to perform their mission, are relevant elements to take into account, as this was done in the EDPB decision 1/2020 regarding Twitter.[9]

Gravity of the infringement

Nature of the processing

Regarding the nature of the processing, the EDPB should include the core activities of the controller as a relevant factor (and not under the purpose of the processing). For example, if the nature of the processing is closely linked to the core activity of the controller, like providing IT services, social media, or electronic communications, which all require large amounts of data, the fine should be increased since the business model of the company is

[8] See § 48 of the Guidelines.
[9] See §151 of the EDPB decision 01/2020.

based on the processing of data. This is because compliance with the GDPR makes even more sense for providers with ancillary data processing activities.[10]

Scope of the processing

Regarding the scope of the processing, we do not see how the local, national or cross-border scope of the processing can have an impact on the calculation of the fine. The range of data processed might be quite large even if the processing is limited to the national borders of a country. Similarly, the scope of the processing can be limited even if the processing is cross-border.

Instead, we would suggest to understand this as the "depth" of the processing operation, which may for example be relevant if a credit ranking agency has not only illegally generated scores about the entire population of a Member State, but has also used extremely sophisticated systems and algorithms to spy on citizens and predict behavior, versus a system that is merely based on past payment history.

Purpose of the processing

The purpose of the processing, in our view, should not relate to the "core activities" of the controller, but rather to the objective pursued by the controller when performing the processing.

Typical examples include monetization of the data, manipulation of people for political, revenge porn, causing intentional discomfort, financial or extremist aims or the monitoring of employees and customers which may have a greater impact on individuals. Usually purposes and intentions such as monetary gain, revenge, acts against minorities, acts against vulnerable groups, malice are traditionally elements that call for higher penalties in national criminal codes and case law.

This may be a very different situation as overreaching processing in the well-meaning interest, the interest of a third party or even in the (alleged) public interest.

Number of data subjects affected

On the number of data subjects affected, whereas it is clearer that the absolute number of data subject should be a relevant factor, we have doubts about the relevance of the ratio between the number of data subjects affected and the total number of data subjects in that context. It seems to us that an absolute number of affected data subjects is the more relevant factor. Using a relative approach would mean that large companies which are processing large amount of data would automatically get away with a lower fine than a smaller company, when violating the rights of the same number of people. Controllers and processors could "process their way out of high fines".

[10] We note that the footnote 20 refers to the nature of the infringement in the Twitter decision, whereas the relevant paragraph in the decision refers to the purpose of the processing.

Level of damages

Regarding the level of damages as an additional criterion, it should be kept in mind that the fine should be independent of any form of indemnification allocated by a court.

We are worried about the reference to Recital 75, which is an introductory recital on the worst case situations when the GDPR is not observed – reminding the controller about the reasons he bears responsibility under Chapter 4 of the GDPR.

Recital 75 GDPR refers situations where the processing may give rise to "secondary damages" (discrimination, identity theft or fraud, financial loss, damage to reputation)[11], while the GDPR is at its core concerned with "primary" damages to the right to data protection alone. It would be problematic if a "mere violation of the GDPR" would be seen as not too grave and DPAs would mainly base their fines on damages to other rights (e.g. the right to property) which are not directly part of their mandate.

We would strongly encourage the EDPB to differentiate between the primarily protected right to data protection alone and any form of secondary damages, which may be protected by other laws in addition to the GDPR.

Intentional or negligent character of the infringement

Concerning the intentional or negligent character of the infringement, we are concerned that the Examples 4 and 5 give a restricted view of what can be an intentional infringement, focusing on a known violation of the law (for example, violating the section of the criminal code prohibiting murder), not a known act (for example, killing a person).

We are not aware of any EU law or national basis for a focus on the known violation of a law instead of an intentional act (for example, triggering a certain processing operation). Instead, it seems to be a common principle in European legal tradition that ignorance of the law is not an excuse (*ignorantia juris non excusat*).

An infringement is clearly still "intentional" even without the formal knowledge of an act being illegal, advice of a DPO or any other legal advice. Otherwise, this would mean that intentional violation of the law would only occur when the perpetrator has been formally informed that the act is illegal. That would lead to a standard for the intentional element that would be too high and difficult to prove (it would be easy for a controller to pretend that it did not know that the act was illegal). In addition, this would incentivize controllers and processors to not get guidance and "play dumb" to avoid fines.

[11] Recital 75 also mentions situations where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Also, the facts described in the second paragraph of Example 4 cannot, in our view, amount to negligence. Negligence is usually defined as behavior that can happen in exceptional cases to an average professionally trained person in the area. We are not sure if acts like "*not abiding by existing policies*" (e.g. not publishing documents on Social Media or not sending passwords to Lebanese princes) or a "*failure to apply technical updates*" (a basic task of any system administrator) could be seen as negligence. The threshold for negligence may be different in case of a single-person controller, that may not be able to understand a "zero day" exploit and happens to be an early victim or a victim of a targeted phishing attack. However failure to adopt a policy or the failure to apply technical measures in line with Article 32 GDPR are however clearly not a case of "negligence". In other words, the lack of actions or omissions may not systematically be seen as negligence. We strongly encourage the EDPB to adapt these elements of the Guidelines.

Finally, the statement according to which "at best, negligence should be considered as neutral" raises questions. Whereas we can understand that, in principle, intentional violations should be fined heavier than negligent violations, we cannot exclude that an intentional violation of the GDPR may lead, under specific circumstances, to a lower fine than in the case of gross negligence.

We very much urge the EDPB to bring this element in line with common principles of European law and national legal traditions, which focus on the intentional act, not the intentional violation of the law.

VI. Starting point for the calculation of fines

In Section 4.2.4, the EDPB proposes a starting amount for the calculation of fines between low, medium and high level of seriousness, leading to respective amounts of 0 -10%; 10-20%, and 20% - 100% of the applicable legal maximum.

These starting points for the calculation of fines are not supported by any reasoning. Moreover, the starting point for low and medium level of seriousness seems to be quite low compared to the range for high level of seriousness which leave a margin of 80 % of the turnover.

We therefore recommend adapting these starting points so that they are better spread out. This should clearly ensure that a "medium" violation is also leading to a "medium" (usually 50%) fine. For example, 0-30 % for low level of seriousness, 30-60 % for medium level of seriousness and 60-70% for high level of seriousness could be more reasonable.

VII. Turnover of the undertaking as an adjustment factor of the fine

We understand that the turnover and size of a company is important to adjust the fine to each specific case, given that the GDPR's € 20 million fine is also applying to individuals that process data outside of Article 2(2)(c) GDPR, non-profits or self-employed persons.

The criteria proposed by the Guidelines to adjust the starting amount make sense in general, but lack of concrete reasoning to justify why these thresholds (turnover) and discounts (from 0.2% to 50 %) were chosen. Such a reasoning would be welcome to understand how the EDPB came up with these numbers, as they seem extremely low.

If we understood the calculation correctly, a company with a turnover of € 2 million per year would pay only € 4.000 to € 8.000 for a medium GPDR violation. This would indeed make violations cheaper than compliance, or indeed just getting legal advice for compliance. We are very concerned about "discounts" of down to 0.2%, which have no basis in law and will be used by controllers and processors against SAs.

The Guidelines also seem to increase a problem created by Article 83 GDPR in general, which is an unfair treatment between controller and processors with high profit margins (low turnover versus profit) compared to sectors with low profit margins (high turnover versus profit). We would strongly encourage the EDPB to use profits as a relevant factor in the "adjustment" factor for reasonable fines, not only turnover.

Overall, we strongly suggest to replace this section with a broader statement on an adjustment for the income and profit of the controller or processor.

At least, the EDPB should highlight extensively (as stated by the Guidelines)[12] that the SA is under no obligation to apply this adjustment if it is not necessary from the point of view of effectiveness, dissuasiveness, and proportionality.

VIII. Aggravating and mitigating factors

We will limit our comments to some of the factors mentioned by the Guidelines.

a. Actions taken by the controller or processor to mitigate the damage suffered by data subjects

Controllers and processors are already under the clear obligation to implement measures to ensure compliance, independently to any damage suffered. Therefore, the actions taken by the controller should only be taken into account in limited circumstances.[13]

We would like to highlight that primarily the damage to the right to data protection must be considered, while secondary damage in relation to other fundamental rights that are separately protected under the CFR (such as the right to property or mental integrity). A duty to mitigate such damages may already be based e.g. on civil law requirements.

On the other hand, situations where the controller does not act at all (by taking at least temporary measures to limit the processing), or where controllers make the situation worse or takes steps to limit any option for data subjects to claim monetary damage (for

[12] See § 68 of the Guidelines.

[13] For example, the controller could stop using a dataset subject to a complaint filed for lack of consent, if there is reasonable doubt about the legality of the processing for all the data subjects whose data are processed by the controller.

example, by deleting the data to which an access has been asked) should definitively be considered as aggravating factors.

b. Degree of responsibility of the controller or processor

This criterion seems to imply that some controllers and processors could be less responsible than others. Articles 25 GDPR should be complied with in any case. Therefore, compliance with these provisions should not be considered as a mitigating factor. Compliance also includes contacts with the DPO (example cited by the Guidelines), who should in any case be involved in any data protection matter (Article 38(1) GDPR).

However, one could understand that in some exceptional circumstances, the controller or the processor could demonstrate that their reaction to a potential violation of the GDPR was followed by effective and appropriate, but for example a joint controller, a processor or a third party has not taken the appropriate measures. In this case, it would be reasonable to allocate penalties according to responsibilities.

Given common industry practices, we would urge the EDPB to highlight that mere contractual "responsibility shifting" cannot be seen as a mitigating factor, but could be seen as not taking responsibility – which would be an aggravating factor.

c. The manner in which the infringement became known to the supervisory authority

Self-reporting non-compliance is usually privileged, in order to encourage controllers and processors to "come clean" and support the investigative work of the SAs. This is clearly a mitigating factor, as long as this is not done when a complaint or procedure is unavoidable or already underway. While informing the DPA is a major factor, a controller or processor may also not be treated as being compliant from the start. Otherwise, there would be a major incentive to break the law and then "neutralize" the GDPR by reporting non-compliance at the end.

Mirroring the privileges for cooperative controllers or processors, the fact that most companies resist the evidence gathering in complaints or ex officio procedures, submit endless irrelevant documents and try to delay the evidence gathering may be seen as elements that will increase a fine. It is in the interest the proper functioning of SAs to highlight this element, as it would clearly speed up and simplify procedures.

d. Adherence to a code of conduct or approved certification mechanisms

We understand that the authors of the GDPR wanted to encourage the use and compliance with Codes of Conducts in the relevant provision of Article 83 GDPR.

We would clarify that only compliance with Codes of Conduct that cover the relevant violation of the GDPR would be a mitigating factor. Compliance with just any Code of Conduct seems to lack any relevant connection a fine over some other violation.

Presumably, a violation of the GDPR will also be a violation of the code of conduct. Thus, the violation would be even more obvious because the controller or processor not only breached the GDPR but also the code of conduct (which is supposed to clarify what conduct to adopt to comply with the GDPR). Such behavior should in principle be considered as an aggravating factor.

In reality, Codes of Conduct are mainly used by the industry to lower the level of protection for data subjects and to clarify uncertainties in the interest of the industry. In such cases, there could be compliance with Codes of Conduct, while there is still a violation of the GDPR. We understand that in such cases compliance with Codes of Conduct may have a presumption of compliance with the law, which could be seen as a mitigating factor.

We hope this clarifies the matter further.

e. Other aggravating and mitigating circumstances

Among the additional circumstances that could be considered as aggravating factors, and as mentioned in the Guidelines (see also Examples 7c and 7d), it is clear that any profit made out of a violation of the GDPR is highly relevant.

In order to assess the extent of the profits made from a violation, SAs should order controllers and processors to share specific details regarding said profits. SAs have the power to obtain all relevant information about the business model underlying a violation of the GDPR. This information would allow the SA to better understand the profit structure of the controller and assess to what extent the violation was profitable for the organisation subject to a fine. This question is obviously linked to the efficiency and deterrence inherent to any fine imposed (see further in the present comments).

We would further suggest to focus on the internal decision making of a controller or processor and ensure that willful violations of the GDPR do not "pay off", a claim that can still be heard from most controllers and processor behind closed doors.

It is crucial that the EDPB sends a clear message that non-compliance is more expensive than compliance.

IX. Legal maximum and corporate liability

We welcome that the criteria suggested by the EDPB to calculate the turnover are the criteria applied in competition law according to a well settled case-law.

We note that the Guidelines suggest using the turnover of the year preceding the final decision of the LSA. The EDPB suggests that this amount should be adapted according to the most up to date financial information available when the draft decision is circulated to the concerned SAs.

However, several years may pass between a draft decision and the final decision of the LSA (or of the EDPB). Turnover may vary significantly over this period of time. Moreover, the calculation of the fines could even be challenged by the controller if it does not mirror

the first assessment made by the SA.[14] To avoid this problem, we urge the LSA and the EDPB to avoid lengthy delays between a draft decision and the final decision.

Moreover, the controllers and processors involved should volunteer this information with the LSA under their duty to cooperate. Instead, the Guidelines refer to the "available information", which implies that the SAs have to proactively look for this information. Of course, the information received from the controllers and processors should always be verified and checked against official documents and financial statements.

X. Effectiveness, proportionality and dissuasiveness

noyb is generally concerned that the core principles of Article 83 GDPR (effectiveness, proportionality and dissuasiveness) get very little room in the Guidelines in comparison with other elements of the provision. It seems to us that the current lack of enforcement would warrant more objective elaboration on how effective and dissuasive enforcement can be undertaken, while observing the general principle of proportionality.

a. Effectiveness

Effective fines are essential to achieving the objectives of the GDPR. There is no for the EDPB to reinvent the wheel. Hundreds of years of research have dealt with how law and society interact, how compliance can be achieved and how companies try to undermine legal frameworks or choose to comply with it. We highly recommend incorporating a section these elements into the Guidelines, including existing basic principles of legal sociology and behavioral studies. Obviously this goes beyond *noyb*'s submission.

Currently we see the following problems on the "effectiveness" element:

- Too often, fines are not imposed at all and procedures are "informally resolved" or a mere reprimand is issued. This is leading to a learning effect, that controllers or processors can expect a free "special invitation to comply" when a case moves before a SA, instead of any serious consequence.
- Equally, penalties that are equal or lower than the cost of compliance, send the message that non-compliance pays off.
- Finally, the low number of fines, in comparison to almost omnipresent GDPR violations make the likeliness of any fine extremely low. In our experience most medium to large controllers or processors have hardly experienced a serious penal procedure before a SA.

The lack of any effective enforcement incentivizes non-compliance or "half-compliance" and in turn creates an ever-growing workload for SAs. In fact controllers are outsourcing compliance to SAs, instead of trying to fully comply with the GDPR from the start.

[14] Some SAs, like the BE SA, have an obligation to share with the controller or processor their intention to impose a fine and the relevant criteria used to assess the level of the fine. Waiting too long before the final decision could make this exercise obsolete.

We encourage the EDPB to insist on this second aspect of fines, especially in cases where the controller or processor intentionally violates the GDPR, and even when the violator complies with the GDPR during the procedure with the SA.

To remain effective, fines must be set taking into account the **cost-benefit analysis** a controller may do before violating the GDPR. It is well-known that controllers and processors weigh the risk of being fined against the potential profit to be made from flouting regulation. The results of this analysis should dictate the dissuasiveness of the fine (see below, under *c.).*

Furthermore, *noyb* is concerned by the magnitude of the fines some SA's have imposed on multinational companies, especially big technology companies (Google, Amazon, Twitter[15]). In the face of these companies' global turnover and reluctance to comply, the fines are comparatively modest. We reach the same conclusion when we compare GDPR fines with fines issued by competition authorities (see for example Amazon, fined € 1.128 billion by the Italian competition authority[16], or Google, fined €2.42 billion[17] and €1.49 billion[18] for abusive practices by the EU Commission).

SAs seem more hesitant than the competition authorities to protect a fundamental right under EU law. We urge the EDPB and the SAs to align the fines imposed for the violation of the GDPR with those imposed under competition law, to which the Guidelines refer several times.

b. Proportionality

According to the Guidelines, SAs can reduce fines on the basis of the principle of the inability to pay as a derivative of the principle of proportionality, which seems to be questionable. After all a controller or processor in a free market society cannot expect to get "social benefits" when violating others' fundamental rights, just because it does not return profits or is not well managed. In fact, it is very common in other areas of the law (tax, social benefits, criminal law) that structurally unlawful undertaking are going out of business when enforcement actions are brought.

Controllers and processors often ask SAs to lower their fines on the basis of losses or lack of profit. However, unlike turnover, profits and losses are not relevant criteria under the text of the GDPR for assessing the magnitude of a fine, except under circumstances where profit was made out of an infringement.

The CJEU has already observed that the mere fact that an undertaking is in poor financial condition or will be after a fine is not objective evidence that the economic viability of the undertaking would be jeopardized.[19]

---

[15] See a list of highest fines under this link : https://www.tessian.com/blog/biggest-gdpr-fines-2020/.
[16] See https://www.agcm.it/media/comunicati-stampa/2021/12/A528-chiusura.
[17] https://ec.europa.eu/commission/presscorner/detail/es/MEMO_17_1785.
[18] See https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.
[19] See §140 of the Guidelines.

The Guidelines also consider that "*a fine reduction may be granted only if the imposition of the fine would jeopardise the economic viability of an undertaking and cause its assets to lose all or most of their value*".[20] However, a connection can always be found between a fine and a loss of value, so loss of value alone cannot in all cases be sufficient justification for reducing a fine. It would be absurd if a controller whose a business model is based on illegal processing of data could rely on this element to ask for a reduction of a fine, since proper enforcement of the GDPR would naturally devalue its core activities. In fact, if the core business is the violation of fundamental rights, the logical consequence is that an undertaking has go out of business to ensure compliance with the GDPR.

Contrary to individual businesses not returning profits, the element of proportionally may play a role when adjusting the cost-benefit analysis in entered sectors with a very high or low profit margin. In certain sectors, such as consumer goods or banking, there is often a very low profit, despite a huge turnover. Other areas, such as IT services usually have a very high profit to turnover ratio. Solely applying the turnover parameter of the GDPR may lead to structurally unfair and therefore disproportionate results, which could be overcome when taking this phenomenon into account on a sector-wide level – instead of a company-specific level.

c. Dissuasiveness

We welcome the reference made by the EDPB to the general and specific deterrence of the fines as a condition for their dissuasiveness. However, as explained above, this element would require **substantially more elaboration** and should feature more prominently, including parameters that are based on existing objective research into behavioral science and legal sociology. We are surprised that this element is only superficially touched in three paragraphs on half a page in the Guidelines.

One phenomenon that seems to be especially relevant the area of data protection, is the fact that many controllers and processors have no moral or intrinsic motivation to comply with the GDPR – other than compliance with traffic rules or the criminal code, which are generally accepted as morally appropriate behavior, or a requirement for the basic functioning of our society. Instead, many undertakings see the GDPR as a moral wrong and have no inner intention to comply. This makes it just the more important that fines are dissuasive, as controllers or processors with this mindset unfortunately have no other realistic reason to comply with the law.

Overall, the **cost-benefit analysis** would have to be the guiding principle on the element of dissuasiveness, by basically adding a calculation that features:

- The saved costs and the earned profits from non-compliance ("benefit")
- The likeliness of any controller or processor in the area being fined ("likeliness")
- A multiplier

[20] See §140 of the Guidelines.

For example:[21] A credit ranking agency does not properly respond to subject access requests, but instead just sends basic information to data subjects, like name and address. All data sources and recipients are not properly documented. The credit scores or the logic are not disclosed to data subjects, as the controller is aware that it does not create objectively correct scores. This allows the controller to save employment costs, as it would have to otherwise employ ten extra people just to deal with GDPR requests. It also ensures that data subjects to not exercise other rights, like the right to erasure, which in turn leads to more data sets that the credit ranking agency can sell to its business customers. Finally, the company saves the costs for changing the system towards a GDPR compliant business model. Overall, only one in ten controllers in this business are fined. To have a positive cost-benefit-ratio and sent the message to other controllers that non-compliance does not pay off, the fine would have to be more than ten times what the controller has saved, to make compliance economically feasible.

We therefore urge the EDPB to add a formula for the "dissuasive" element in Article 83 GDPR, which is centered on a **cost-benefit-analysis including costs saved, profits made and likeliness of a fine**. It seems to us that the current Guidelines do not give enough weight to the core principles of Article 83 GDPR, but instead overinflate the details of the provision.

We thank the EDPB for the opportunity to provide comments, hope that our feedback was useful for the EDPB, and remain at the disposal of its members for any questions they may have.

[21] Based on a real case in Austria.