Spolek pro ochranu osobních údajů

Comments on the EDPB draft of Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR

We welcome the opportunity to comment on the EDPB draft Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR ("**Guidelines**"), which have been published for public consultation.

Our Association values the EDPB's effort to bring more consistency and predictability into the sanctioning practice of supervisory authorities across the EU. A common and transparent framework for deciding when a fine is the appropriate tool, and when another corrective power is sufficient, is in the interest of supervisory authorities, controllers, processors, and data subjects alike.

We particularly appreciate that the Guidelines expressly build on the case-law of the Court of Justice of the EU, according to which only an infringement committed intentionally or negligently may give rise to an administrative fine (judgments of 5 December 2023, C-683/21 Nacionalinis visuomenės sveikatos centras and C-807/21 Deutsche Wohnen).

General comments

However, we must point out that, in our view, the Guidelines are overly rigid in certain respects and that this approach may further diminish the EU's attractiveness as a destination for investment in the data economy. Some of the EDPB's conclusions also raise doubts as to whether fundamental principles of due process and the principle of legality have been duly taken into account.

One example is the requirement of culpability referred to above: while the Guidelines acknowledge the wording of the GDPR and the case-law of the Court of Justice of the EU, they effectively negate that requirement (see para. 49) by relying merely on Opinions of Advocates General, which suggest that liability is, in effect, a form of strict liability. In doing so, the EDPB assumes a quasi-legislative role, interpreting the text of the legislation in a manner contrary to both its purpose and its express provisions (see also Article 83(2)(d) GDPR). It is possible that the EDPB intended this statement similarly to AG to apply only to cases where the controller should have been aware that it was infringing the GDPR. However, the wording used unfortunately suggests instead that this is intended as a general conclusion applicable to Article 83 as a whole.

The GDPR deliberately provides supervisory authorities with a broad toolbox of corrective powers in Article 58(2), of which an administrative fine is only one. Under Article 83(1) and (2) GDPR, a fine must be effective, proportionate and dissuasive in each individual case and is to be imposed "depending on the circumstances of each individual case", in addition to or instead of other measures.

From the practical experience of our members (data protection officers and other data professionals in both the private and public sectors), we are concerned that the draft, read as a whole, tilts this balance. Several of its building blocks (the starting point for the decision, the approach to culpability and the very limited room for mitigating circumstances) each move the assessment towards a fine. Taken together, they may leave little space for the individual assessment the GDPR requires.

We believe this is not only a legal issue. An enforcement framework that does not distinguish between organisations which invest in compliance and those which do not, gives little incentive for responsible behaviour. As a form of so-called performance-based regulation, the GDPR leaves controllers considerable discretion as to how to comply with its requirements. This inevitably entails a risk of erroneous assessments and non-compliant processing. Against this background, it should be of particular importance whether the controller concerned acted in good faith and had an effective

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address 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.: +420 730 677 644

compliance system in place, even if that system failed to prevent the particular infringement. If these circumstances are not duly taken into account, controllers will be discouraged from introducing new solutions, especially in the digital economy. This could further weaken the EU's already limited position in the digital economy.

We set out our detailed observations below.

Specific comments

1. Interim measures (Section 3.6, para. 32)

We consider it appropriate that interim measures are linked to the need to “provisionally protect the right of data subjects”, as stated in paragraph 32. However, it would be useful for the EDPB to elaborate further and expressly acknowledge the need to protect the interests of the controller concerned, and thus of European industry, as well. Those interests may also be significantly affected by interim measures, and an inappropriately chosen interim measure may cause irreparable harm to the controller concerned. Particularly in the current period of crisis, such measures should therefore be chosen with caution and their proportionality should always be duly assessed.

2. Starting point for the decision on a fine (Section 5.1, para. 57; Section 5.3.3, para. 119)

Paragraph 57 introduces "a strong presumption to impose an administrative fine" for every infringement that does not qualify as minor. We find it difficult to reconcile such a presumption with Article 83(2) GDPR and with the Guidelines' own acknowledgment that the decision to fine lies within the discretion of the supervisory authority. A presumption shifts the burden: the authority would effectively need reasons not to fine, rather than reasons to fine. Given how broadly "non-minor" may be understood, this could affect a large number of cases involving primarily formal deficiencies, for example in documentation.

We suggest replacing the presumption with a neutral formulation requiring the supervisory authority to choose the corrective measure that is appropriate in light of all circumstances of the case. Section 3.4 on reprimands could be complemented with illustrative scenarios in which a reprimand or an order under Article 58(2)(d) GDPR is the proportionate response – for instance, where the infringement resulted from an honest misreading of an unsettled legal question, caused no damage to data subjects and was promptly corrected after being identified.

3. Culpability and the relevance of EDPB guidance (Section 4.3, paras. 49–50)

As noted above, this is one of the fundamental problems with the Guidelines as a whole. We would also like to emphasise several further points.

We agree that, under the case-law cited above, it is not necessary for the controller to have been aware that it was infringing the GDPR. However, the draft goes further by suggesting that an error is in principle avoidable whenever EDPB guidance on the topic exists. This would, in our view, give soft law an effect it does not have. EDPB guidelines are not binding, they are frequently revised, and – as our Association has noted in several previous consultations – their wording sometimes leaves room for differing readings, which is also reflected in divergent practices of national supervisory authorities.

We therefore propose that the Guidelines limit the relevance of EDPB guidance for the assessment of negligence to guidance that (i) had been adopted in its final version before the conduct in question took place and (ii) addressed the specific situation clearly. Negligence should remain a matter to be established by the supervisory authority on the facts of each case.

4. Examples 2 and 4. We do not consider Example 2 to be particularly well chosen. In particular, it is unclear whether the expert concerned acts as a processor (in which case no separate legal basis for

the transfer of data would be required) or as a controller. As regards Example 4, we would welcome the EDPB expressly addressing the situation where the legal opinion in question is, by contrast, consistent with the prevailing views in the legal literature.

5. The reference in paragraph 68 to "potentially affected" data subjects is not entirely clear to us. If the EDPB has in mind a situation in which it is difficult to determine the number of data subjects affected because the controller concerned does not cooperate adequately, such an approach may be justified. It should not, however, allow hypothetical cases that might arise to be taken into account. Clarification on this point would be very helpful.

6. Reliance on legal analysis (Section 4.3, para. 50 and Example 4; Section 5.2.3, paras. 71–72)

Example 4 sets out a number of situations in which reliance on legal advice is not to be considered in the controller's favour. Controllers, and their data protection officers, are routinely confronted with questions to which the GDPR, the case-law and the guidance do not provide a definite answer. Where the controller has analysed such a question carefully, considered the opposing views and recorded its reasoning, this is exactly the kind of behaviour the accountability principle in Article 5(2) GDPR is meant to encourage. Disregarding such analysis entirely risks turning it into a mere formality.

We would welcome the Guidelines clarifying that a reasoned and documented assessment made in good faith may be taken into account when assessing the degree of culpability, and distinguishing between situations of genuine legal uncertainty and situations in which a controller knowingly accepts the risk of infringement. This may be particularly relevant to newly introduced processing operations in the evolving digital economy, where even after carrying out a DPIA, it may not always be straightforward for controllers to design their processing arrangements correctly in every respect. Here, too, good faith should be a significant mitigating factor. We must draw attention to a practical issue we frequently encounter. While controllers design such new processing operations at a time when no relevant sources of guidance are available, supervisory authorities may decide whether to impose a fine only several years later, with the benefit of backsight regarding all the weaknesses of those arrangements (which may not have been apparent from the outset), as well as newly published studies, academic articles and other materials. It is therefore essential to assess such cases from the perspective of the controller's circumstances at the time the processing was introduced as well. The positive effect that an appreciation of the practical challenges associated with introducing new technologies could have on technology companies' willingness to adopt innovative approaches hardly needs emphasising.

The Guidelines should also confirm that controllers cannot be expected to disclose communications with their legal advisers covered by professional secrecy in order to demonstrate that they acted with due care.

7. Responsibility for processing carried out by processors (Section 4.2, paras. 41–43)

Although we acknowledge that the Court of Justice of the EU interprets a controller's responsibility for the activities of "its" processor very broadly, as noted in the Guidelines, we must nevertheless point out that these conclusions are at times overly categorical, particularly in view of the requirement of fault expressly laid down in the GDPR. In many cases, it will be appropriate to hold a controller responsible for processing carried out on its behalf. In other cases, however, particularly where the controller has taken all measures that could reasonably be required of it to prevent the infringement (including implementing a robust compliance system and conducting audits), the Court's conclusions appear excessively strict for the purposes of administrative fines, including in light of the principles of due process and legality.

For the sake of completeness, we note that the quotation from the judgment in Case C-741/21 cited in paragraph 24 concerns compensation for damage under Article 82 GDPR, rather than the imposition of fines.

We support the statement in the Guidelines that a controller cannot be held liable where a processor processes data for its own purposes or otherwise disregards the controller's instructions. The subsequent reference to a possible liability of the controller, for instance under Article 32 GDPR, should however be framed carefully. The Court of Justice in Case C-683/21 confirmed that a controller may be fined for processing carried out by a processor only to the extent that the controller can be held responsible for that processing.

We suggest clarifying that any liability of the controller in such cases requires the supervisory authority to identify and establish a specific shortcoming on the part of the controller itself, and that the mere fact that a processor or another third party acted unlawfully is not sufficient to conclude that the controller's measures were inappropriate.

It would also be useful for the EDPB to elaborate on acts by a controller's own employees that go beyond the scope of their duties or instructions, and on the implications of such conduct for the controller's liability.

8. Weight of mitigating circumstances (Sections 5.2.4 to 5.2.10)

Article 83(2) GDPR lists a range of circumstances to be taken into account, many of which can operate in the controller's favour. The draft, however, gives them very limited practical effect: compliance measures are relevant "only in exceptional circumstances", while cooperation with the supervisory authority, the absence of previous infringements and compliance with previously ordered measures are in principle not to be considered as mitigating (paras. 77, 88, 90–91 and 99).

In our view, this risks placing a controller that has built a functioning data protection management system, informed the authority on its own initiative and remedied the situation quickly, in essentially the same position as a controller that has done none of this. We recommend that the Guidelines allow these circumstances to be given real weight where justified by the facts of the case (see also paras. 73–74 and 95–96). As our Association has already noted in the context of data breach notifications, management is in some cases reluctant to report a breach for fear that the controller will subsequently be exposed to sanctions. An approach that gives little weight to openness towards supervisory authorities may reinforce this reluctance, to the detriment of data subjects. It is also important to take into account the somewhat uneasy relationship between the obligation to notify personal data breaches and the principle of nemo tenetur. This should also be reflected in the assessment, and a breach notification, even if submitted in compliance with the obligation under Article 33 GDPR, should ordinarily be treated as a mitigating circumstance.

9. Classification of infringements as minor (Section 5.1, para. 56; Section 5.2.2, paras. 66–69; Section 5.2.13, Examples 6–10)

The practical examples of minor infringements in the Guidelines involve exclusively small entities. Combined with assessment criteria that are closely linked to the scale of processing (such as the number of data subjects potentially concerned or the systemic character of an infringement), this may create the impression that the minor category is effectively reserved for small organisations. We note in this respect that the size of an organisation is already reflected in the maximum amount of the fine, which is calculated on the basis of total worldwide annual turnover; it should not, in addition, determine whether a fine is imposed at all. Moreover, as we noted in our position paper on the evaluation of the GDPR, a specific project within a large organisation may well be run with resources comparable to those of a small business.

We would therefore welcome confirmation that an infringement may be classified as minor irrespective of the size of the controller, with the decisive factors being the actual risks and consequences for data subjects. The set of examples could be broadened accordingly, for instance by scenarios involving a larger controller where a short-lived technical error affected only a limited number of data subjects and

Spolek pro ochranu osobních údajů

was promptly corrected, or where an outdated contact detail in the information provided to data subjects was rectified as soon as it was identified.

10. Profitability as aggravating circumstance (Section 5.2.12, para. 106)

We strongly caution against the EDPB's somewhat oversimplified approach to the profits earned by controllers. It is essential to distinguish carefully between profits that are causally linked to a deliberate infringement of the GDPR and profits arising in other circumstances. In many cases, controllers may act in good faith in an effort to comply with the GDPR, and any profit earned may be an unintended consequence of a possible infringement. Care should be taken to avoid creating the impression that the EU is a bloc that penalises profitable companies.

We thank the EDPB for the opportunity to share our views on the draft Guidelines and for its continued work on clarifying the application of the GDPR.

Prague, 12.11.2026

JUDr. Vladan Rámiš, Ph.D.
Chairman of the Committee
Data Protection Association

Mgr. Jana Pattynová, LL.M.
Member of the Committee
Data Protection Association