PIERSTONE

tel +420 224 234 958
www.pierstone.com

Perlová 371/5, Prague 1
Czech Republic

12 November 2026

European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
Belgium

Submitted via the EDPB public consultation procedure

Comments on draft Guidelines 04/2026 on administrative fines

PIERSTONE appreciates the opportunity to take part in the public consultation on draft Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR, adopted on 17 September 2026 (the "Draft Guidelines").

We advise controllers and processors of all sizes, from start-ups to large cloud and technology providers, on GDPR compliance and on proceedings before supervisory authorities. The observations below draw on that experience.

We support the EDPB's aim of making the choice between a fine and the other corrective powers more consistent and predictable across the EEA. We also welcome the clear statement, in line with the Court of Justice's judgments of 5 December 2023 in C-683/21 Nacionalinis visuomenės sveikatos centras and C-807/21 Deutsche Wohnen, that a fine requires an infringement committed intentionally or negligently.

Our concern is the cumulative effect of the methodology. Article 58(2) GDPR gives supervisory authorities a range of corrective tools, and Article 83(1) and (2) GDPR require that any fine be effective, proportionate and dissuasive and be decided "depending on the circumstances of each individual case", in addition to or instead of other measures. Several elements of the Draft Guidelines each push the assessment towards a fine.

In practice, these elements concern the reading of culpability, the narrow room left for mitigating factors and the starting presumption in favour of a fine. Taken together, they risk replacing case-by-case judgement with something close to a default outcome. This also matters for policy reasons. A framework that treats an organisation with a mature compliance programme much like one that has invested nothing gives businesses weak incentives to do the right thing.

We have grouped our comments in two parts. Part A covers the legal preconditions for a fine. Part B covers the decision whether to fine.

PIERSTONE is an international alliance of lawyers registered by the Brussels Bar Association.
PIERSTONE s.r.o., advokátní kancelář, Na Příkopě 392/9 a 393/11, Prague 1, ID: 27136710, Municipal Court in Prague reg. C 119770.

Part A: Preconditions for a fine

A.1 Controller liability for the conduct of processors (Section 4.2, paragraphs 42 and 43)

We agree with the Draft Guidelines that the attribution to the controller is broken where a processor uses personal data for its own purposes or acts outside the controller's instructions. The following sentence, which notes that the controller may nonetheless remain liable on a separate basis such as Article 32 GDPR, needs more precise wording.

In C-683/21, the Court of Justice held that a controller can be fined for processing carried out by a processor only where that processing can be attributed to the controller. To keep paragraph 43 consistent with that ruling, we recommend that the EDPB state expressly that:

(a) the supervisory authority must identify and prove a specific failing of the controller itself, for example inadequate security measures or insufficient oversight of the processor; and

(b) the fact that a processor or another third party acted unlawfully is not, on its own, enough to conclude that the controller's technical and organisational measures were inappropriate.

A.2 Negligence and the role of EDPB guidance (Section 4.3, paragraphs 49 and 50)

We do not dispute that, under the case-law cited, a controller need not have known that it was infringing the GDPR for its conduct to be negligent. Paragraph 50, however, goes a step further. It treats any error as avoidable, and therefore at least negligent, whenever EDPB guidance on the subject exists.

In our view, this gives soft law a legal effect it does not have. EDPB guidelines are not binding. They are regularly updated, and their wording can support more than one reading, which is visible in the differing practices of national supervisory authorities. A rule that automatically converts the existence of guidance into a finding of negligence would let non-binding texts decide an element of liability that the GDPR leaves to the facts.

We therefore suggest that EDPB guidance be relevant to negligence only where it (i) had been adopted in final form before the conduct in question and (ii) clearly addressed the specific situation at issue. Even then, negligence should remain something the supervisory authority establishes on the facts of each case.

A.3 Good-faith reliance on legal analysis (Section 4.3, paragraph 50 and Example 4; Section 5.2.3, paragraphs 71 and 72)

Example 4 lists several situations in which legal advice relied on by the controller is to be given no weight in its favour. Our experience is that controllers and their data protection officers often face questions that the GDPR, the case-law and the guidance do not answer definitively.

Where a controller has examined such a question carefully, weighed the competing views and recorded its reasoning, it is doing what the accountability principle in Article 5(2) GDPR asks of it. Should such an assessment be disregarded entirely once an infringement has been established, controllers would have little incentive to carry it out with due care, and there is a risk that it would be reduced to a mere formality.

We would welcome three clarifications in the Draft Guidelines:

(a) a reasoned, documented assessment made in good faith may be taken into account when assessing the degree of culpability under Article 83(2)(b) GDPR;

(b) a distinction should be drawn between genuine legal uncertainty and cases where a controller knowingly accepts the risk of infringing the GDPR; and

(c) controllers cannot be expected to disclose communications with their legal advisers protected by professional secrecy in order to show that they acted with due care.

Part B: Deciding whether to impose a fine

B.1 Minor infringements and the size of the controller (Section 5.1, paragraph 56; Section 5.2.2, paragraphs 66 to 69; Section 5.2.13, Examples 6 to 10)

Every practical example of a minor infringement in Section 5.2.13 involves a small organisation: an SME, a small sports club or a small telecommunications company. Several of the criteria in Section 5.2.2 also depend on the scale of processing, such as the number of data subjects potentially affected and the systemic character of an infringement. Read together, these could suggest that only small organisations can benefit from the minor-infringement category.

The size of an organisation is already reflected in the maximum fine, which is calculated on total worldwide annual turnover. Size should not also decide whether a fine is imposed at all. In addition, a single project or business unit within a large group may operate with resources no greater than those of a small company.

We recommend that the EDPB confirm that an infringement can be minor regardless of the controller's size, and that the decisive factors are the actual risks and consequences for data subjects. The examples could be widened to include a larger controller, for instance:

(a) a short-lived technical error that affected only a limited number of data subjects and was promptly corrected; or

(b) an outdated contact detail in the information provided to data subjects, corrected as soon as it was identified.

B.2 The practical weight of mitigating factors (Sections 5.2.4 to 5.2.10)

Article 83(2) GDPR lists many circumstances that supervisory authorities must consider, and several of them can work in the controller's favour. The Draft Guidelines, however, leave these factors with very little practical effect. Under paragraph 77, compliance measures count as mitigating "only in exceptional circumstances". Under paragraphs 88, 90, 91 and 99, cooperation with the supervisory authority, a clean record and compliance with previously ordered measures are in principle not mitigating.

The result is that a controller that has built a working data protection management system, approached the supervisory authority on its own initiative and remedied the problem quickly could end up in much the same position as a controller that has done none of these things. We recommend that the Draft Guidelines allow these circumstances to carry real weight where the facts justify it.

B.3 The presumption in favour of a fine and the role of reprimands (Section 5.1, paragraph 57; Section 5.3.3, paragraph 119; Section 3.4)

Paragraph 57 establishes "a strong presumption to impose an administrative fine" for every infringement that is not minor.

We find this presumption hard to reconcile with Article 83(2) GDPR and with paragraph 9 of the Draft Guidelines itself, which recognises that the imposition of fines is at the discretion of

the supervisory authority. A presumption reverses the logic of the assessment: the supervisory authority would in effect need reasons not to fine, rather than reasons to fine. Because the category of non-minor infringements may be read broadly, the presumption could reach many cases that concern mainly formal shortcomings, such as gaps in documentation.

We propose replacing the presumption with neutral wording that requires the supervisory authority to select the corrective measure that is appropriate in light of all the circumstances of the case. Section 3.4 on reprimands could support this by giving examples where a reprimand, or an order under Article 58(2)(d) GDPR, is the proportionate response. One example would be an infringement that arose from an honest misreading of an unsettled legal question, caused no harm to data subjects and was corrected promptly once identified.

We thank the EDPB for considering these observations and for its continued efforts on clarifying the application of the GDPR.

Jana Pattynová, Partner
Karina Matevosjanová, Senior Associate
PIERSTONE