Response to the public consultation: EDPB Guidelines 04/2026 on the power to impose administrative fines under the GDPR

We have taken note of the European Data Protection Board (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 has been circulated for public consultation until 13th November, 2026. We are grateful for the opportunity to provide comments.

Inter alia, we welcome in particular the EDPB's position in paragraph 55, according to which "*when deciding whether to impose an administrative fine in each individual case the factors in Article 83(2)(a) to (k) GDPR shall be taken into account*". We strongly agree that "*the factors in Article 83(2)(a) to (k) GDPR therefore serve to ensure that each infringement is assessed on the basis of all the relevant individual circumstances and that the objectives pursued by the system of penalties provided for in the GDPR are achieved*".

The power to impose fines is only one of the many tasks and powers granted to Supervisory Authorities (SAs) under articles 57 and 58 of the GDPR. Advising and accompanying organisations to understand the requirements of the law and the application of the rules in specific contexts should be prioritised over enforcement, since continued constructive engagement between SAs and organisations better enables effective protection of personal data and of data subjects on the ground.

Most companies see GDPR compliance as a key element of a trustworthy relationship with their clients (both in BtoB and on BtoC relationships) and strive to act responsibly. Therefore, it is also important that SAs look at the full picture and put the alleged infringement into perspective *vis-à-vis* the overall state of compliance of the organisation.

Areas of concern

While we support the objective of consistent enforcement, we would like to point out the following areas of concerns that will be elaborated later in our response:

1. **Fines are not the silver bullet to effective data protection:** Fines sit on an equal footing with nine other corrective tools under Article 58(2) GDPR; non-monetary corrective measures must be properly calibrated and tailored across all organisation sizes, and SAs should prioritise corrective orders and constructive dialogue over automatic financial penalties.

2. **Overbroad fines exposure and culpability (Step 3):** The draft Guidelines themselves recognise that the GDPR administrative fines meet the Engel criteria.[1] It follows that Articles 48 and 49 of the Charter should inform the culpability assessment at this step; the draft sets the negligence bar so low that it effectively introduces strict liability.

3. **Assessing the gravity of the infringement:** Thresholds for qualifying infringements as recurring or systemic (such as 5 complaints), as well as blanket classifications of data categories and economic gain, are unbalanced and risk disproportionate fining.

4. **Incentives for compliance (Step 4):** Genuine accountability measures, privacy-enhancing technologies ('PETs'), and self-reporting must serve as meaningful mitigating factors, while prior infringements must be strictly bounded.

5. **Keep harmonisation as a north star:** Predictability, transparency, and safeguards: SAs must be subject to an explicit duty to state reasons regarding culpability and the choice of corrective measures, protect legitimate expectations, ensure transparent calculations, and prevent cumulative penalisation (*ne bis in idem*).

The proposed approach seems rather conservative, which does not align with the open approach announced in the Helsinki Statement.[2] We therefore urge the EDPB to take into account these concerns and the suggestions hereunder.

1) Fines are not the silver bullet to effective data protection

Administrative fines must not become the automatic default remedy. Non-monetary corrective measures (reprimands, orders, and processing bans) must be properly calibrated and tailored across all organisation sizes. For the vast majority of businesses operating in the EU, non-monetary corrective powers under Article 58(2) GDPR are sufficient to secure compliance and should be properly calibrated:

- **Equal statutory footing:** Paragraph 18 provides that fines constitute a "central element" of the GDPR enforcement regime. However, Article 58(2) GDPR, which sets out the corrective powers of SAs, does not establish any hierarchy among the available corrective measures, all of which stand on an equal footing. Fines are merely one instrument among ten others and are, in fact, listed second to last: this suggests that

[1] European Court of Human Rights, Judgment of 8 June 1976, *Engel and Others v. the Netherland*s, Applications nos. 5100/71; 5101/71; 5102/71; 5103/71; 5370/72.
[2] European Data Protection Board (EDPB), *The Helsinki Statement on enhanced clarity, support and engagement: A fundamental rights approach to innovation and competitiveness*, adopted on 2 July 2025. Available at: https://www.edpb.europa.eu/documents/reports-statements-and-letters/the-helsinki-statement-on-enhanced-clarity-support-and_en

fines should not necessarily be regarded as the primary or preferred or by-default enforcement tool.

- **Broadening standalone reprimands beyond strictly "minor" breaches (paragraphs 25–26):** The draft Guidelines read Recital 148 too restrictively by limiting standalone reprimands (without a fine) to "minor" infringements or disproportionate burdens on natural persons. Recital 148 is illustrative, not exhaustive. The final Guidelines should confirm that a reprimand alone is also an appropriate outcome where the controller's degree of negligence is low, or where the infringement caused no tangible damage to data subjects.
- **Prioritising and specifying compliance orders:** In most cases, requiring an organisation to adjust its practices within a specified timeframe (e.g. through a compliance order) is likely to produce a more positive and immediate impact on compliance and the protection of personal data than imposing a fine *ab initio*. While a fine may incentivise behavioural changes, it does not, in and of itself, immediately enhance the level of personal data protection. Enforcement measures and fines should therefore be reserved for clearly intentional or repeated infringements, demonstrating a persistent unwillingness to comply with the applicable rules. We would accordingly request the EDPB to give greater consideration to this aspect in the final Guidelines and adjust the wording of paragraph 18 accordingly. Additionally, compliance orders must be specified and issued only where necessary (paragraphs 27–30). For businesses (especially Small and medium-sized enterprises (SMEs) without large in-house legal teams) vague orders to "*bring processing operations into compliance*" create severe legal uncertainty. In line with Article 58(2)(d) ("specified manner and within a specified period"), the final Guidelines should require SAs to specify the concrete steps expected of the controller. They should also confirm that a compliance order is unnecessary where the organisation has already ended or adjusted the relevant processing and informed the SA, or where there is no reason to doubt that it will act on the SA's finding.
- **Calibrating outcomes across organisation sizes:** The draft examples suggest that large organisations can rarely commit a minor infringement**:** indeed, several Step 4 factors (e.g., scope, the number of data subjects "potentially affected," and systemic nature) scale with organisational size. Read together, this suggests that a "lighter" outcome is rare for large companies, if ever. We ask the EDPB to explicitly clarify that organisational size alone does not disqualify an infringement from being considered "minor", and to include illustrative examples where low-impact or procedural breaches by larger entities are resolved through non-monetary measures, such as standalone reprimands under Recital 148, rather than fines.

2) Overbroad fines exposure and culpability (Step 3)

The draft contains several problematic positions that tend towards an overreach in fines across all businesses:

- **Culpability (Step 3):** CJEU case law (*Deutsche Wohnen*[3] and *NVSC*)[4] confirms that the imposition of a fine requires an intentional or negligent infringement. However, the draft Guidelines sets the threshold for establishing negligence so low that it risks being met in virtually every case. In particular, the proposed standard of carelessness appears overly broad, suggesting that it is sufficient for an organisation to have been in a position to know that its conduct was unlawful. Our main concerns are:
    a) **Elevation of non-binding guidelines to strict liability:** The statement that the mere existence of EDPB guidelines renders any error avoidable and therefore, at the very least, negligent (paragraph 50) is insufficiently balanced, particularly where the relevant guidance is non-binding, still in draft form, was published after the conduct in question, or is ambiguous and open to different interpretations. This approach effectively turns a non-binding guidance into a *de facto* binding standard, without restricting its relevance to guidelines that are final, in force at the time of the conduct, and directly applicable to the specific circumstances of the case.
    b) **Supervisory authority divergences:** Treating a departure from the known position of any supervisory authority as evidence of negligence, even where supervisory authorities themselves hold divergent views, including within the one-stop-shop mechanism, risks imposing an unreasonable standard of foreseeability on organisations.
    c) **Documented legal advice:** Treating the existence of documented legal advice as evidence that an organisation was aware of an infringement, rather than recognising it as an indication of due diligence and good-faith efforts to ensure compliance, risks discouraging organisations from seeking legal advice and documenting their compliance efforts.
- **Engel criteria and Charter rights:** The EDPB itself acknowledges that GDPR fines are criminal in nature under the *Engel* criteria. Articles 48 (presumption of innocence) and 49 (principles of legality and proportionality of criminal offences and penalties) of the Charter of Fundamental Rights ('Charter') should therefore inform this step.
- **Negligence as a proven precondition and protection against retroactive standards (paragraphs 47–53):** Under CJEU case law (*Deutsche Wohnen* and *NVSC*) and Article 48 of the Charter, negligence is a distinct precondition where the burden of proof rests on the SA. Fault cannot be presumed automatically whenever an infringement is unintentional, particularly where an organisation genuinely believed its practices complied with the GDPR. SAs must prove foreseeability based on contemporaneous facts, resolving any doubt in the controller's favour. The draft Guidelines fail to address common situations where the law, SA practice, or EDPB guidance leaves room for interpretation or does not anticipate a specific use case. Where an organisation and an SA arrive at differing interpretations at the enforcement stage, the final Guidelines should exclude a finding of fault, presume good faith, and exclude the imposition of a fine.

[3] Judgment of the Court (Grand Chamber) of 5 December 2023, *Deutsche Wohnen SE v Staatsanwaltschaft Berlin*, C-807/21, EU:C:2023:950.
[4] Judgment of the Court (Grand Chamber) of 5 December 2023, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos*, C-683/21, EU:C:2023:949.

Crucially, to protect legal certainty and prevent retroactive penalisation, this presumption of good faith must strictly apply where the processing activity predated the publication of EDPB guidelines specifically addressing that use case.

- **Reversing the burden via presumptions:** The draft's proposal that, where an infringement is not minor, "*there is a strong presumption to impose an administrative fine*" effectively reverses the underlying question from "*should a fine be imposed?*" to "*can the SA justify not imposing one?*". This risks making fines the default response, potentially extending their application to routine administrative paperwork or procedural deficiencies.
- **Supply-chain liability where a processor acts outside instructions (paragraph 43):** Businesses across the digital economy rely on external processors and technical vendors. In *NVSC* (paragraph 85), the CJEU confirmed that a controller's liability cannot extend to processing carried out by a processor for its own purposes or outside the controller's framework and instructions, in which case Article 28(10) GDPR qualifies the processor as a controller in its own right. While paragraph 42 acknowledges this principle, paragraph 43 appears to suggest, without further explanation, that controllers may nevertheless remain liable even where the attribution of responsibility is disrupted. This apparent inconsistency with *NVSC* should be addressed and the wording clarified accordingly.

3) Assessing the gravity of the infringement

The draft's criteria for evaluating the gravity of an infringement under Article 83(2) GDPR require recalibration:

- **Thresholds for systemic infringements (paragraph 88):** Paragraph 88 contains an example of how an infringement may evolve from a minor incident to a recurring infringement. However, the proposed threshold appears disproportionately low, with only five complaints being sufficient to illustrate such an evolution. The EDPB should take into account the fact that complaints may actually originate from competitors, disgruntled employees or from organisations acting with nefarious intentions. While receiving five complaints may qualify as a minor incident, they should not, in themselves, constitute a reasonable benchmark for establishing a systemic infringement. We therefore ask the EDPB to reconsider this example.
- **Categorisation of data (paragraph 92):** We do not agree that location data should be considered a near-sensitive category of data without any nuance. The paragraph should remove the reference to "location data" or, at the very least, should clarify "precise location data". The same can be said for transaction overviews, which should be linked to the categories of data covered by Articles 9 and 10 GDPR.
- **Amount vs. substantive harm of data (paragraph 93):** In Paragraph 93, the EDPB considers the amount of data regarding each data subject as a relevant factor in determining the gravity of an infringement. We request the EDPB to reconsider this

statement, as the volume of data is often an incorrect indicator of the actual harm caused. For instance, the disclosure of one illness (e.g., cancer) of a named data subject to unauthorised recipients can be much more harmful than the collection of browsing events and measurement data for advertising purposes through cookie IDs, where there is no possibility to link the data to the individuals behind the screen. The assessment should therefore focus on the nature and sensitivity of the data and the actual or potential impact on data subjects, rather than relying primarily on volume.

- **Economic gain (paragraph 106):** The EDPB considers that if a controller has profited or has had an economic gain from an infringement, this may constitute a strong indication that the infringement is not minor. However, the relevance of the financial benefits should always be considered based on the specific circumstances of the case and the type of infringement. As currently drafted, this principle risks being applied too broadly, potentially subjecting otherwise minor infringements to fines simply because the controller operates in an economic context. Such an approach could also lead to a disproportionate assessment of business activities in the context of data economy and AI development, contrary to the principle of technological neutrality underpinning the GDPR. We ask the EDPB to reconsider this paragraph.

4) Incentives for compliance (Step 4)

The draft sets an unreasonably high bar for mitigating factors, thereby undermining the risk-based approach:

- **Incentives for compliance (Step 4):** The draft sets an overly restrictive standard for recognising mitigating circumstances. In paragraph 77, compliance measures are considered mitigating "*only in exceptional circumstances*" where the controller has gone "*above and beyond*" its legal obligations; ordinary cooperation is not recognised as a mitigating factor; a clean enforcement record carries no mitigating weight; and compliance with previous orders is similarly disregarded. This risks placing organisations with mature and well-established compliance programmes on substantially the same footing as those with no meaningful compliance measures in place. More broadly, under the draft, accountability measures (Articles 24, 25 and 32 GDPR), cooperation and compliance with previous orders are only recognised as mitigating factors where they exceed existing legal obligations. Conversely, previous infringements may be taken into account irrespective of their subject matter or the time elapsed, including those established by other supervisory authorities. This approach is inconsistent with the risk-based approach and undermines the incentive for organisations to maintain robust compliance frameworks. We would therefore suggest that:
    - Accountability measures should be recognised as a genuine mitigating factor, rather than being considered relevant only "in exceptional circumstances" where an organisation exceeds statutory baselines;

- Previous infringements should be limited to those that are final, relevant, and reasonably recent, preventing perpetual exposure across unrelated processing activities.
- Remedial measures implemented before a final decision should be credited under Article 83(2)(c) in proportion to their effect (and assessed only against criteria disclosed in advance), so organisations are incentivised to improve their practices while an inquiry is ongoing.

- **Privacy Enhancing Technologies and pseudonymisation (paragraph 76):** The EDPB should be more favourable in recognising that pseudonymised data can serve as a mitigating factor in enforcement proceedings. The current drafting is overly defensive, stating that this can only be applied in exceptional circumstances. With such restrictive wording, the EDPB fails to incentivise the use of pseudonymisation and other PETs that can effectively strengthen the protection of personal data. It is crucial that organisations understand how the investments required to implement these PETs will be taken into account in case of enforcement. Recognising more clearly that these technologies can lead to enhancing data protection in practice, together with the fact that they will be considered by SAs in case of enforcement, will encourage their adoption, which in turn will increase the overall level of personal data protection. We ask the EDPB to review the wording of this paragraph to make the statement in a more constructive manner.
- **Self-reporting and leniency (paragraph 96):** The EDPB considers that the notification to the SA of an infringement by a controller on its own motion can be considered as a mitigating factor (paragraph 96). In order to make this even more effective, the EDPB should also mention that, depending on the circumstances of the case, this could also preempt the imposition of a fine altogether. In this respect, the EDPB could draw inspiration from the leniency mechanisms established under EU competition law, where voluntary disclosure and cooperation may result in immunity from, or a reduction of, financial penalties.

5) Keep harmonisation as a north star: Predictability, transparency, and safeguards

As mentioned in the introduction of the draft Guidelines (paragraph 10), consistent enforcement of the data protection rules by the SAs is central to ensuring a harmonised data protection regime. This should remain the guiding principle of the Guidelines. Consequently, they should encourage SAs to provide transparency in their methodology on whether to impose a fine and to calculate its amount. Where a supervisory authority decides to impose an administrative fine, the Guidelines must ensure that the resulting penalty is proportionate, transparent, and free from double counting, in accordance with Articles 83(1) and (8) GDPR and Articles 41, 47, and 49–50 of the Charter:

- **Predictability and reasoning:** The Guidelines should establish explicit duty to give reasons on both culpability and the choice of corrective measure. In particular, SAs must

provide case-specific justifications explaining why non-monetary corrective measures under Article 58(2) were deemed insufficient before resorting to an administrative fine. They should also recognise legitimate expectations where an authority remained silent or had accepted a given interpretation.

- **Properly bounding temporary and permanent processing bans (paragraphs 31–34):** Suspending data processing can halt a company's core commercial operations overnight. As paragraph 32 notes, a temporary ban under Article 58(2)(f) is an interim measure prior to establishing the facts and infringement; the Guidelines should confirm that it cannot be imposed in a final decision or combined with an Article 58(2)(d) compliance order.
- **Positive framing of procedural transparency:** Instead of taking a defensive and negative approach, emphasising that SAs are not obliged to follow the steps that are not applicable in a specific case or are not obliged to provide reasoning on aspects of the guidelines that are not applicable, the Guidelines should be drafted more positively to clarify that:
    - SAs must follow the steps applicable in a given case and provide explanations and full transparency on their reasoning on aspects of the Guidelines that are relevant to the case. Where a fine is imposed, this should explain why a fine is imposed, how its amount has been calculated, and how aggravating and mitigating factors have been taken into account.
    - Even on steps or aspects that are not applicable, SAs are strongly encouraged to provide reasoning and transparency for the purpose of enabling increased consistency in the enforcement of data protection rules.
- **Case-specific proportionality and deterrence reasoning (paragraphs 108–113):** Fining decisions should not rely on boilerplate statements that a penalty is effective, proportionate, and dissuasive. SAs must provide case-specific explanations on why a lower monetary amount would not achieve the intended objective, how any accompanying reprimand or compliance order reduces the fine needed, how general deterrence translates into the specific figure chosen, and what justifies selecting any amount above the minimum of a proposed fining range.
- **Transparent calculation methodology and reference turnover:** To guarantee legal certainty and effective judicial review, a SA decision must clearly state why a fine is imposed for each infringement, the baseline starting amount, and the direction and approximate weight of each aggravating and mitigating adjustment under Article 83(2). In addition, the final Guidelines should clarify that the "preceding financial year" under Article 83(4)–(6) refers to the company's turnover before the infringement (or, at the latest, before the inquiry opened), so that controllers are not prejudiced by a SA's delay in concluding multi-year proceedings.
- **Preventing cumulative penalisation (*ne bis in idem*) and applying the Article 83(3) cap:** A single business or website workflow often engages multiple GDPR provisions at once. Penalising the same underlying conduct more than once through separate findings under different articles, or counting the same factor twice (such as considering data categories both under the gravity assessment in Article 83(2)(a) and under Article 83(2)(g)) risks violating Article 50 of the Charter and the principle of *ne bis in idem*. SAs

must isolate the conduct attributable to each provision and avoid any overlap in the calculation of the fine. Finally, the final Guidelines should confirm that under Article 83(3) GDPR, where multiple infringements arise from the same or linked processing operations, the total fine is capped at the fine set for the gravest infringement rather than aggregating separate fines up to the statutory maximum.

***

We thank you in advance for your consideration of these concerns and suggestions, and hope they will contribute to meaningful improvements to the methodology for determining whether an administrative fine should be imposed, either in addition to or instead of the other corrective measures available under Article 58(2) GDPR.