Contribution to the EDPB Public Consultation

on the Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR (v1.0, 17 September 2026)

Observations from the perspective of a Lawyer and Data Protection Officer:
Submitted by: Avv. Francesco Luongo — Cassazionista, Lawyer, Data Protection Officer
Contribution category: DPO / Individual
Country: Italy — www.linkedin.com/in/francesco-luongo
Sector: Professional and technical activities; public-law professional bodies

1. Premise and Position of the Contributor

This contribution is submitted in a personal and professional capacity, drawing on practical experience as a lawyer and as the appointed Data Protection Officer of a professional body governed by public law.

It does not represent the formal position of any public body or client.

The observations below focus in particular on the role of the Data Protection Officer within the enforcement methodology proposed by the Guidelines.

The draft correctly requires supervisory authorities, as a preliminary step, to identify the party that can legally be fined for the infringement. Paragraphs 40–46 identify the addressee of the relevant obligation, such as the controller, processor, certification body or monitoring body.

However, the Guidelines subsequently refer to the involvement of the Data Protection Officer both as evidence of organisational conduct and as a possible indicator of persistent compliance deficiencies. In particular, paragraph 78 refers to possible “contact with the Data Protection Officer”, while paragraph 85 refers to infringements arising from having ignored the advice of the DPO.

These references make it particularly important to preserve a clear distinction between the advisory and monitoring role of the DPO and the legal responsibility of the controller or processor for GDPR compliance.

2. General Assessment

The proposed five-step methodology provides a clear and useful framework for distinguishing between the existence of an infringement, the possibility of imposing an administrative fine, the element of culpability, the seriousness of the infringement and the choice of the appropriate corrective measure.

The distinction between the first three steps, concerning the legal preconditions for a fine, and the subsequent assessment of whether a fine should actually be imposed is particularly valuable.

The Guidelines also appropriately recognise that the different corrective powers under Article 58(2) GDPR pursue different purposes. Some measures primarily aim to restore compliance, whereas administrative fines also have a punitive and deterrent function.

The following observations are therefore intended to refine the methodology rather than question its general structure.

In particular, the final Guidelines could usefully clarify the position of the Data Protection Officer so that effective DPO involvement is properly recognised as part of organisational accountability without creating any unintended transfer of responsibility from the controller or processor to the DPO.

3. Step 2 — Clarifying that the DPO Is Not the Addressee of the Controller's or Processor's Compliance Obligations

Paragraph 40 correctly states that liability for an infringement depends on identifying the addressee of the specific provision that has been breached. Depending on the provision concerned, this may be the controller, processor, certification body or monitoring body.

The Guidelines could usefully make explicit that the Data Protection Officer does not become the addressee of the controller's or processor's substantive GDPR obligations merely by performing the functions assigned under Articles 38 and 39 GDPR.

The DPO informs and advises, monitors compliance, provides advice on data protection impact assessments, cooperates with supervisory authorities and acts as a contact point. The DPO does not, by virtue of that role, determine the purposes and essential means of processing, nor does the DPO replace the controller or processor in discharging their respective obligations under the GDPR.

This distinction is particularly important in enforcement proceedings.

The involvement of a DPO in a processing activity should therefore not be interpreted as transferring responsibility for the underlying compliance decision to the DPO.

At the same time, the controller or processor should not be able to rely on the existence or advice of a DPO as a mechanism for transferring its own responsibility.

Recommendation: the Board should consider adding an express clarification to Section 4.2 stating that a Data Protection Officer acting within the functions assigned under Articles 38 and 39 GDPR is not personally responsible for the controller's or processor's compliance with the GDPR and cannot be treated, solely by virtue of performing the DPO function, as the addressee of obligations resting on the controller or processor.

This clarification would be without prejudice to obligations expressly applicable to the DPO, including confidentiality under Article 38(5) GDPR, or to liability arising under other applicable law from conduct outside the statutory DPO function, including where such conduct involves a separate organisational role entailing decision-making over the purposes and essential means of processing.

4. Step 3 — DPO Advice and the Assessment of Negligence

The Guidelines state that an administrative fine requires an intentional or negligent infringement and explain that the threshold for establishing negligence may be relatively low. The decisive question is whether the addressee was in a position to know that their conduct was unlawful.

Examples 4(a)–(c) also correctly demonstrate that external or internal legal advice does not automatically exculpate a controller.

The position of the DPO nevertheless deserves separate consideration.

A DPO is not simply an internal or external legal adviser. The function is expressly established and protected by the GDPR and forms part of the organisation's accountability framework.

Seeking DPO advice should not provide an automatic safe harbour. The controller or processor remains responsible for the final decision and cannot justify clearly unlawful conduct merely by referring to the DPO.

However, effective and timely involvement of the DPO may constitute relevant evidence of the level of organisational due diligence exercised by the controller or processor.

This may be particularly important where the legal question is genuinely complex or unsettled and where the controller has:

- provided the DPO with complete and accurate information;
- involved the DPO before the relevant decision was taken;
- considered the DPO's advice in good faith, and, where it decided not to follow that advice, documented the reasons for doing so;
- documented the decision-making process; and
- adopted a reasoned position after assessing the identified risks.

In such circumstances, DPO involvement should not eliminate responsibility, but it may be relevant when assessing the degree of negligence.

Recommendation: Section 4.3 should clarify that consultation with the DPO neither transfers responsibility nor automatically excludes negligence, but may constitute one of the objective circumstances relevant to assessing the level of due diligence exercised by the controller or processor.

5. Article 83(2)(d) — Effective DPO Involvement as Evidence Relevant to Organisational Accountability

Paragraphs 75–78 concern the degree of responsibility of the controller or processor and require supervisory authorities to consider the technical and organisational measures implemented under Articles 24, 25 and 32 GDPR.

Paragraph 78 expressly provides that relevant documentation may include evidence of "contact with the Data Protection Officer".

The concept of mere "contact" may be too narrow.

The existence of a formally appointed DPO should not, in itself, constitute a mitigating circumstance where designation is required by law.

What may instead be relevant is whether the DPO function operated effectively in practice.

For example, a supervisory authority could consider whether:

- the DPO was involved properly and in a timely manner;
- the DPO had access to the information necessary to perform the role;
- the DPO had adequate resources and organisational independence;
- the DPO was able to report directly to the highest management level;
- relevant recommendations were issued and documented;
- management actually considered those recommendations before taking its decision.

These factors may help distinguish an isolated operational error occurring within an otherwise functioning accountability framework from a systemic failure of governance.

Recommendation: paragraph 78 could refer to the "effective and timely involvement of the Data Protection Officer, where applicable", rather than merely to "contact" with the DPO.

The Guidelines should also clarify that such evidence relates to the organisational accountability of the controller or processor and does not create personal responsibility for the DPO.

6. Paragraph 85 — The Consequences of Disregarding DPO Advice

Paragraph 85 refers to previous infringements committed in the same manner as potentially indicative of persistent organisational problems and gives as an example infringements arising from having ignored the advice of the Data Protection Officer.

This is an important point, but further clarification would improve legal certainty.

DPO advice is not equivalent to an order issued by a supervisory authority and is not legally binding on the controller or processor.

The controller or processor retains the authority — and corresponding responsibility — to make the final decision.

Therefore, departing from DPO advice should not automatically constitute an aggravating circumstance.

The relevant question should rather be whether the organisational decision-making process demonstrates an effective accountability framework.

Where DPO advice identifies a clear and significant compliance risk, is properly documented and is communicated to the appropriate decision-making level, repeated disregard of that advice without adequate assessment or justification may legitimately indicate a systemic organisational deficiency.

Conversely, management may in some cases reach a different legal or operational conclusion after genuinely considering the DPO's advice. Where management departs from the DPO's advice, the existence of a documented and reasoned assessment may therefore be particularly relevant in distinguishing a legitimate exercise of management responsibility from a systemic disregard of the DPO function.

The decisive element should therefore be the behaviour of the controller or processor, rather than the mere existence of disagreement with the DPO.

Recommendation: paragraph 85 should clarify that disregard of DPO advice may be relevant where it evidences a repeated or systemic failure of the controller or processor to maintain an effective compliance framework, while confirming that DPO advice is not binding and that responsibility for the final processing decision remains with the controller or processor.

7. DPO-Triggered Remediation as a Positive Accountability Mechanism

The Guidelines appropriately recognise the importance of measures taken by controllers and processors to mitigate the consequences of an infringement.

Paragraphs 73–74 emphasise the relevance of timeliness and provide that measures spontaneously implemented before the controller or processor becomes aware of a supervisory investigation are more likely to constitute mitigating factors.

The same principle is developed in paragraphs 114–117, where the Guidelines recognise that, in some circumstances, it may not be appropriate, necessary or proportionate to exercise any corrective power where the controller has autonomously brought the infringement to an end and prevented recurrence.

This reasoning could be usefully connected to the preventive role of the DPO.

An effective accountability system should be capable of detecting deficiencies internally rather than only after a complaint, data breach investigation or supervisory intervention.

The DPO's monitoring activities under Article 39(1)(b) GDPR, together with internal audits, periodic reviews and staff reporting mechanisms, can contribute directly to identifying compliance failures.

Where the DPO detects a deficiency, reports it to the controller or processor and the organisation promptly adopts effective remedial measures before supervisory intervention, this should be recognised as evidence that the internal accountability system is functioning.

The responsibility for the infringement and for the remedial decision nevertheless remains with the controller or processor.

Recommendation: the Board could consider adding a practical example in which a compliance deficiency is identified through DPO monitoring activities and promptly corrected by the controller before supervisory intervention, illustrating how such conduct may be relevant under Articles 83(2)(c), 83(2)(d) and, where appropriate, Article 83(2)(k).

8. Small Public-Law Bodies and Proportionality

The Guidelines correctly acknowledge that Member States may determine whether and to what extent administrative fines may be imposed on public authorities and bodies.

They also recognise that proportionality requires consideration of the individual circumstances of the case and that, where several equally appropriate penalties are available, the least onerous measure should be selected.

A practical example concerning small public-law bodies could further improve the usefulness of the Guidelines.

Professional bodies and comparable non-economic public entities may process significant categories of personal data while operating with limited staffing, technical resources and budgets.

Their public-law or non-profit nature cannot justify a lower substantive standard of data protection.

However, in deciding whether an administrative fine is proportionate, the supervisory authority may legitimately have regard to the overall institutional context, including:

- the scale and resources of the organisation;
- the absence or presence of economic gain;
- the nature of the statutory functions performed;
- the impact of the sanction on the performance of public-interest functions;
- the effectiveness of the internal compliance framework, including, where applicable, an appropriately involved and independent Data Protection Officer;
- the speed and effectiveness of remedial measures.

These circumstances should not create immunity from enforcement. They may nevertheless be relevant to choosing between an administrative fine and another corrective measure capable of achieving an equally effective and dissuasive outcome.

Recommendation: the Guidelines could include a practical example concerning a small public-law or non-profit body in order to illustrate the application of the proportionality principle without lowering the level of protection guaranteed by the GDPR.

9. The DPO as an Accountability Safeguard, Not a Transfer Point for Liability

The Guidelines provide an opportunity to reinforce an important structural principle of the GDPR.

A strong DPO function does not replace accountable management.

Its purpose is precisely the opposite: to support accountability by identifying risks, advising the organisation, monitoring compliance, escalating unresolved issues and cooperating with supervisory authorities.

Where these mechanisms function effectively, DPO involvement may provide relevant evidence concerning organisational due diligence, degree of responsibility, mitigation and proportionality.

Where management fails to involve the DPO, prevents the DPO from carrying out the statutory functions, disregards material recommendations without adequate assessment or attempts to transfer responsibility for organisational decisions to the DPO, such conduct should remain attributable to the controller or processor.

The enforcement framework should therefore preserve a clear distinction: the DPO advises and monitors; the controller or processor remains responsible for the decisions and obligations falling within its respective role.

10. Conclusion

The Guidelines provide a valuable framework for increasing consistency in the exercise of supervisory authorities' corrective powers throughout the EEA.

The proposed methodology appropriately distinguishes between the legal conditions for imposing a fine, the assessment of culpability, the seriousness of the infringement and the proportionality of the corrective response.

The final Guidelines would nevertheless benefit from a clearer treatment of the role of the Data Protection Officer.

In particular, they should make clear that effective DPO involvement may be relevant evidence of organisational due diligence and accountability, but does not transfer responsibility for GDPR compliance from the controller or processor to the DPO.

At the same time, the DPO should not become a formal shield behind which controllers or processors seek to avoid their own responsibilities.

A clear recognition of the DPO as an independent advisory and monitoring safeguard — rather than as a decision-maker or substitute for accountable management — would strengthen legal certainty, DPO independence and the overall effectiveness of the GDPR enforcement framework.

The contributor remains available to provide further detail or practical examples on any of the points raised, and thanks the Board for the opportunity to contribute to this consultation.

Yours faithfully, **Avv. Francesco Luongo**