13 November 2026

EBF_047110

EBF response to the European Data Protection Board's consultation on the draft Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR

The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's (EDPB) consultation on the draft Guidelines on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR, hereinafter – the Guidelines. In particular, we would like to draw the EDPB's attention on a number of points that merit further consideration in the final version of the Guidelines.

We would **welcome clarification under Paragraphs 41-45 on liability allocation in complex banking group structures and M&A scenarios**. In particular, additional guidance would be helpful regarding controller-processor chains, intra-group service arrangements, parent company liability, corporate succession following mergers, acquisitions or internal reorganisations. Clarifying these aspects would contribute to greater legal certainty and help ensure that **liability and culpability assessments remain linked to the specific role, conduct and degree of control exercised by the entity concerned**, rather than being inferred solely from group membership, contractual relationships or succession arrangements. This would be particularly valuable in the context of large cross-border banking groups operating through complex organisational structures.

We would also welcome if the Guidelines could provide practical **examples illustrating the application of liability allocation**, particularly in complex controller-processor arrangements, and **the assessment of minor infringements**. Such examples would support a more consistent and predictable application of the Guidelines across sectors and jurisdictions.

Paragraph 50 states that "[...] *where EDPB Guidelines exist, an error is always to be considered avoidable and therefore at least negligent*". This statement risks giving non-binding EDPB guidance a de facto binding effect and fails to account for practical complexities, such as guidelines remaining under consultation for extended period, the absence of established practice, uncertainty about the interpretation of the law, and conflicting or divergent national requirements from (sectoral) supervisors. **EDPB Guidelines should be treated as a relevant factor in an individual assessment of negligence, rather than automatically establishing it.** Moreover, reliance on national DPA guidance, sectoral supervisory requirements, as well as genuine legal uncertainty or an interpretation confirmed or left open by the CJEU, should be considered as **mitigating factors under Article 83(2)(b) and (k) GDPR**.

We would also like to raise concerns at the approach taken in Paragraph 50, Examples 4a-4c and Paragraph 85. Read together, these provisions appear to be at odds with the GDPR accountability framework, as they risk discouraging organisations

from documenting their privacy assessments and governance processes. In particular, they could create a situation where:

(i) documented legal assessments can become evidence of negligence because they demonstrate that alternative interpretations were identified and discussed (cf. Example 4);

(ii) documented DPO advice may later be used as an aggravating element where management ultimately adopts a different position (cf. Paragraph 85); and

(iii) identified risks, doubts and mitigation discussions become factors weighing against the controller (cf. Paragraph 50).

Articles 5(2), 24, 35 and 39 GDPR encourage controllers to identify risks, document assessments, consult the DPO, challenge assumptions and keep evidence of decision-making. Organizations that diligently perform DPIAs, maintain governance records and document disagreements should not find themselves in a less favourable position than organizations that do not document such analyses.

We therefore recommend clarifying that the existence of documented governance processes, DPIAs, legal assessments, risk analyses and DPO consultations should generally be regarded as evidence of a mature accountability framework and therefore be considered as mitigating factors. The mere fact that a risk was identified, discussed and documented should not, in itself, be used to establish negligence or aggravation.

At a more granular level, we would like to raise the following considerations on Example 4 and Paragraph 85:

- **Example 4a** suggests that relying on an opinion that cites opposing legal views demonstrates awareness and may therefore establish negligence. Even if this may not exclude negligence, **we recommend recognising a reasoned, documented good-faith legal assessment as a relevant mitigating factor**.
- **Example 4b** implies that internal legal advice departing from or opposing a DPA's "known opinion" constitutes negligence. The Guidelines should **distinguish between reasoned disagreement with a DPA position and a disregard for that position**.
- **Example 4c** expects legal advice to be documented and produced. This risks turning a balanced, documented risk assessment required under Articles 5(2) and 24 into evidence against the controller. The expectation to produce legal advice also raises concerns regarding the confidentiality of in-house legal advice under applicable national legislation. We recommend clarifying that no adverse inference should be drawn from non-disclosure of confidential legal advice.
- **Paragraph 85** discusses infringements "*arising as a consequence of having ignored the advice of the Data Protection Officer.*" We note that WP243 'Guidelines on DPOs' accepts divergence where reasons are documented. As drafted, however, this paragraph discourages governance models in which legal and DPO views are weighed against each other. We therefore recommend **limiting this interpretation to divergences that are undocumented or unreasoned**.

Paragraphs 65-68 and 92 address the aggravating factors under Article 83(2) GDPR. We highlight that the cumulative effect of these factors – namely, that the processing constitutes a core activity, it involves a large number of data subjects and the processing of Articles 9-10 and financial data – is likely to mean that, in practice, nearly all infringements by a bank will be considered as non-minor from the outset. **We therefore recommend:**

1. **Assessing financial data by actual exposure (disclosure, dissemination, misuse potential) rather than by category.**
2. **Giving the ratio criterion in paragraph 68 real weight, so that a low error rate across high volumes points to a non-systemic failure.**
3. **Adding a minor-infringement example involving a large controller.**

We would also welcome an explicit clarification that DPAs should focus their assessment on the nature and scale of a controller's activities and not rely on its turnover, as this may be a poor proxy for the scale of a company's data processing activities. If overall turnover significantly overstates the scale of the company's relevant activities, the authority should be able to reduce the starting point substantially to ensure proportionality. This clarification should follow from the reasoning underlying Examples 6a and 6b of the Guidelines 04/2022.

As regards the mitigating factors (cf. Paragraphs 77, 88, 90, 99), **the Guidelines give limited weight to the existence of a robust privacy control framework**. In regulated organizations, such as banks, compliance is necessarily risk-based, and no framework can completely eliminate isolated human errors. Where an organization can demonstrate mature governance, effective controls, monitoring, training, DPO oversight and prompt remediation, an isolated failure should not automatically lead to the conclusion that the infringement is not minor. **We therefore recommend, at Step 4, expressly recognising the robustness of the compliance framework and the isolated character of the failure as relevant to the "minor infringement" assessment**, irrespective of their treatment for calculation purposes.

Finally, we would like to recall that one incident may trigger multiple enforcement framework (e.g., GDPR, DORA, NIS2, AML, MiFID). Although **Footnote 8** refers to relevant CJEU case law (e.g. CJEU 22 March 2022, bpost, C 117/20), it does so only for the Engel criteria ("punitive purpose and severity of a penalty in the broad sense"), and does not address the *ne bis in idem* principle. **We therefore recommend clarifying that, under Article 83(2)(k) GDPR, measures or sanctions imposed by other authorities in respect of the same facts must be taken into account, including in the choice between a reprimand and a fine.** This clarification should refer to Article 50 of the EU Charter and the relevant CJEU case law.

ENDS

For more information:
Rachele Ceraulo
Policy Adviser – Data & Digital Finance
r.ceraulo@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significantmajority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth

www.ebf.eu @EBFeu