PUBLIC CONSULTATION COMMENTS

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

Juan Emmanuel Delva Benavides
Jorge Antonio Leos Navarro
Alejandro Paul García Hernández
Iván Said González López

Research Group UDEG-CA-1236 “Law and Technology” · University of Guadalajara, Mexico

The comments express the academic views of their authors and do not represent an official position of the University of Guadalajara.

November 2026

LEGAL FRAMEWORK

This collective submission addresses Article 58(2) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), concerning corrective powers; Article 83(1), requiring administrative fines to be effective, proportionate and dissuasive; Article 83(2), concerning the individual assessment and possible combination of measures; Article 83(5)(e) and Article 83(6), concerning failures to comply with relevant orders; Article 83(7), concerning public authorities; and Recitals 26, 129 and 148. References to sections and numbered paragraphs below concern the EDPB's draft Guidelines 04/2026, version 1.0, adopted on 17 September 2026.

GENERAL OBSERVATION

These comments welcome the EDPB's effort to distinguish the legal prerequisites for imposing an administrative fine from the subsequent assessment of the appropriate corrective response. A methodology that makes enforcement decisions more consistent is valuable, provided that it does not substitute rigid presumptions for the case-specific reasoning required by Articles 58(2) and 83 GDPR. The following proposals focus on the operational relationship between punitive and restorative measures, the interpretation of technological risk, and the reasoning needed to make enforcement decisions intelligible and reviewable.

1. CLARIFY THE RELATIONSHIP BETWEEN STEP 4 AND STEP 5 (PARAGRAPHS 9–12, 108–121)

The Guidelines distinguish minor from non-minor infringements at step 4 by reference to Article 83(2)(a)–(k) GDPR and Recital 148, before applying the requirements of Article 83(1) GDPR at step 5. That distinction is useful, but the “general rule” against fines for minor infringements (paragraphs 56–57 and 115) and the “strong presumption” in favour of a fine for non-minor infringements (paragraph 57) can be misread as an automatic decision rule. This risk is especially relevant when the underlying violation is technically limited but causes lasting harm, or is widespread but remediable through measures tailored to eliminate an unlawful practice.

Recommendation: state expressly, in the overview and at the start of section 5.3, that classification under step 4 informs but does not determine the outcome under step 5. Authorities should explain why the chosen combination of measures is necessary in the individual case, including when they depart from the general approach. Consider including a short decision template distinguishing the

seriousness assessment, preventive or restorative objectives, punitive or deterrent objectives, and the proportionality of the overall response.

2. AVOID DOUBLE COUNTING WHEN MEASURES ARE COMBINED (PARAGRAPHS 16–20 AND 97–100)

The Guidelines correctly recognise that corrective powers under Article 58(2) GDPR may pursue different purposes and that Article 83(2) GDPR permits an administrative fine to be imposed in addition to, or instead of, other corrective measures. They also acknowledge that the same non-compliant behaviour cannot be punished twice (paragraph 100). Additional operational guidance would help authorities distinguish legitimate cumulative enforcement from duplicative reliance on the same fact or conduct.

Recommendation: include an illustrative matrix identifying the distinct purpose of each selected measure, the conduct or risk addressed, its prospective or retrospective effect, and the relevant proportionality considerations. Where failure to obey an earlier order is relevant to the compliance assessment under Article 83(2)(i) GDPR and may constitute a distinct infringement under Article 83(5)(e) or Article 83(6) GDPR, authorities should identify the factual basis of each assessment and explain how they have prevented impermissible duplication. The aim is not to prohibit cumulative measures, but to make their combined rationale transparent.

3. REVISE EXAMPLE 7: HASHED CONTACT DATA ARE NOT NECESSARILY UNUSABLE (SECTION 5.2.13)

Example 7, in Section 5.2.13 of the draft Guidelines, describes an infringement of Article 32(1) GDPR involving the unintentional transfer, through a social media tracking pixel, of hashed contact details (email addresses and telephone numbers) of approximately 50,000 users to the social media provider over a two-year period. It describes the transferred data as “hashed, and thus unusable” in support of the conclusion that the infringement was minor. This proposition is too categorical. Hashing does not, by itself, establish anonymisation or practical unusability. Article 4(5) GDPR provides the legal definition of pseudonymisation, while Recital 26 calls for an assessment of means reasonably likely to be used to identify a person. The extent to which email addresses or telephone numbers remain linkable depends on factors such as the algorithm, whether a salt or keyed method was used, the entropy of the source data, the availability of comparison datasets, the recipient's information and the reasonably likely means of re-identification. The EDPB's own work points the same way. Guidelines 01/2025 on Pseudonymisation explain that, where the transformation is known, an unkeyed hash can be reversed by hashing candidate values and matching the results (paragraph 88 and footnote 23), and they call for transformations that involve secret information of sufficient entropy (paragraphs 88–90). The draft Guidelines 02/2026 on Anonymisation, in turn, treat a dataset containing pseudonyms that can easily be reverse engineered as not anonymous (paragraph 50). Email addresses and telephone numbers are typical candidates for such reversal, because the space of plausible values is limited, and in Example 7 the recipient is a social media provider, a type of recipient that commonly holds the same identifiers for its own users. Outside the Union, the United States Federal Trade Commission has likewise warned that hashes are not anonymous and can still be used to identify users.

Recommendation: replace the categorical assertion with a fact-dependent finding supported by a technical assessment in the hypothetical scenario. If the example is intended to illustrate low-risk pseudonymised data, specify the relevant safeguards and the factual reasons why further identification was unlikely. If those facts cannot be supplied, present risk as uncertain rather than treating hashing as dispositive. This clarification would make the example more consistent with the GDPR's

distinction between anonymised and pseudonymised data and avoid encouraging the mistaken inference that hashed personal identifiers automatically fall outside meaningful privacy risk.

4. EXPLAIN HOW REPEATED OR AUTOMATED INCIDENTS AFFECT SERIOUSNESS (EXAMPLES 5 AND 10)

Examples 5 and 10 illustrate how repeated infringements may reveal a systemic failure rather than isolated minor mistakes, a distinction relevant to the nature, duration, responsibility and previous-infringement factors in Article 83(2)(a), Article 83(2)(d) and Article 83(2)(e) GDPR. This principle is increasingly important where a processing configuration, automated workflow or third-party integration can generate many similar violations before an organisation detects them. The number of affected individuals, persistence over time, foreseeability and recurrence after remedial intervention may all be relevant, but should not be reduced to a fixed numerical threshold.

Recommendation: add an example in which an apparently modest single incident is traced to a repeatable technical configuration. Explain how an authority can move from incident-level analysis to systemic seriousness while still distinguishing recurrence, evidence of organisational negligence and the actual consequences for data subjects. Such an example would improve guidance for AI-enabled and other high-volume processing environments without creating a novel statutory offence.

5. ADDRESS PUBLIC AUTHORITIES AND NATIONAL LEGAL VARIATION (PARAGRAPH 2; PARAGRAPHS 119–120)

Paragraph 2 recognises Article 83(7) GDPR, under which Member States may determine whether and to what extent administrative fines can be imposed on public authorities and bodies. Paragraph 120 appropriately notes that a reprimand or another corrective measure may be used where national law precludes a fine. A clearer account of the enforcement objective in those circumstances would improve the practical value of the Guidelines.

Recommendation: include a compact example explaining how the authority evaluates effectiveness, necessity and proportionality where monetary penalties against a public body are unavailable. The emphasis should be on enforceable compliance orders, verification of remedial action and consequences of continued non-compliance. The Guidelines should explicitly distinguish this EU-law issue from comparative frameworks outside the European Economic Area, which may offer useful scholarly perspectives but are not sources of binding interpretation of the GDPR.

6. MAKE REASONING AND REMEDIATION VERIFIABLE (PARAGRAPHS 12 AND 108–121)

The Guidelines recognise that invoking the methodology does not replace the duty to state reasons in an individual case. Article 83(1) GDPR sets the effectiveness, proportionality and dissuasiveness criteria, while Article 58(2) GDPR governs the available corrective powers; see also the judgment of the Court of Justice of 26 September 2024, Land Hessen, C-768/21, EU:C:2024:785, paragraph 42, on which the Guidelines themselves rely. This safeguard should be operationalised without imposing a rigid form inconsistent with national procedures. In particular, an authority's explanation should make clear whether a remedy aims to stop ongoing processing, correct existing consequences, prevent recurrence or deter future violations, and why a fine adds or does not add material value to that set of measures.

Recommendation: attach a non-binding checklist for reasoned enforcement decisions: (a) conduct and legal provision established; (b) actor's role and the required mental element; (c) gravity and context under Article 83(2); (d) corrective measures considered and their respective purposes; (e) cumulative impact and risk of duplicative punishment; (f) reasons for imposing, reducing or omitting a fine;

and (g) relevant compliance-monitoring or review arrangements. This would support consistency, procedural fairness and public accountability while allowing authorities to adapt the explanation to the individual file.

7. CORRECT INTERNAL CROSS-REFERENCES IN THE STEP 5 DISCUSSION

Paragraphs 114 and 118 direct readers to Section 4.1 when referring to the assessment of whether an infringement is minor at step 4. Section 4.1 addresses step 1, whereas the step 4 assessment is developed in Section 5.2. Recommendation: update both cross-references to Section 5.2 (or the more precise relevant subsection), so that the methodological roadmap can be followed without ambiguity.

CONCLUSION

The proposed additions would preserve the EDPB's five-step approach while making the proportionality assessment more transparent, technically sound and operationally usable, consistently with Article 83(1) and Article 83(2) GDPR. In particular, the clarification concerning hashed contact data warrants attention because a simplified technical assumption in an enforcement example can unintentionally influence how authorities and organisations assess the seriousness of infringements.

PRIMARY LEGAL AND POLICY REFERENCES

European Data Protection Board. (2026). Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR (Version 1.0, adopted 17 September 2026). https://www.edpb.europa.eu/system/files/2026-09/edpb_guidelines_202604_imposing-administrative-fines_v1_en_0.pdf

Public consultation: https://www.edpb.europa.eu/public-consultations/guidelines-042026-on-the-application-of-the-power-to-impose-administrative_en

European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), in particular Article 4(5), Article 58(2), Article 83(1), Article 83(2), Article 83(5)(e), Article 83(6) and Article 83(7), and Recitals 26, 129 and 148. Official consolidated legal text: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Court of Justice of the European Union. (2024). Judgment of 26 September 2024, Land Hessen, C-768/21, EU:C:2024:785.

European Data Protection Board. (2025). Guidelines 01/2025 on Pseudonymisation (version for public consultation, adopted 16 January 2025), in particular paragraphs 88–90 and footnote 23. https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

European Data Protection Board. (2026). Guidelines 02/2026 on Anonymisation (Version 1.0, adopted 7 July 2026, version for public consultation), paragraph 50. https://www.edpb.europa.eu/system/files/2026-09/edpb_guidelines_202602_anonymisation_v1_en_0.pdf

Federal Trade Commission, Office of Technology. (2024, 24 July). No, hashing still doesn't make your data anonymous. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous