Asylum Research&Global Assistance

Administrative fines and effective remedies

Response to EDPB Guidelines 04/2026

European Data Protection Board

21 October 2026 | France

ARGA — Asylum Research & Global Assistance supports enforcement that is effective, proportionate and dissuasive, with reasoned decisions and meaningful procedural safeguards. Our contribution concerns the impact of data misuse on individuals, attribution of responsibility, evidentiary quality and the relationship between sanctions and corrective action. The recommendations address the consultation draft adopted on 17 September 2026.

1 Preserve the sequence of the assessment

The five-step structure is useful if each step remains distinct. The final guidance should make explicit that establishing an infringement, identifying the appropriate addressee, establishing intention or negligence and deciding on a sanction require their own reasons. The desirability of deterrence must not substitute for evidence of the relevant infringement and responsibility.

For complex processing chains, the decision should identify the actor's actual role, the processing operation, the breached duty and the evidence connecting that actor to the breach. Paragraphs 42–43 should be illustrated with cases distinguishing a processor acting within instructions, a processor exceeding them and a controller's separate failures of selection or oversight. Contractual labels should neither shield actual responsibility nor justify automatic liability for every participant.

We recommend examples involving AI-assisted systems, but the mere use of AI should not be treated as an infringement or an aggravating factor in itself. The authority should establish the relevant facts: for example, the actual collection, use, disclosure, accuracy failure or failure to honour an applicable right.

2 Keep culpability and individual assessment explicit

We support the requirement to establish intention or negligence. The final guidance should explain the evidential reasoning required when awareness, organisational omissions or ignored warnings are relied upon. A documented compliance system can be relevant evidence, but its existence alone does not prove reasonable conduct; nor does a failed control automatically establish intentional misconduct.

The strong presumption discussed in paragraphs 55–57 for non-minor infringements should be accompanied by an express safeguard that it does not reverse the burden of establishing the infringement or culpability. The authority should still give an individualised explanation of why a fine is appropriate, taking account of the relevant Article 83 factors and the available corrective powers.

ARGA recommends separating three questions in the reasons: why the infringement is or is not minor; why a fine or another measure is appropriate; and how the amount is determined under the applicable framework. This would improve reviewability and avoid collapsing distinct assessments into a single conclusion about severity.

3 Assess consequences beyond aggregate numbers

A small number of affected people does not necessarily indicate minor consequences. The guidance should include examples where inaccurate or improperly disclosed information can have substantial effects on a person's safety, reputation or access to essential services. Examples concerning contested criminal allegations or asylum-related information would illuminate the importance of context without creating automatic sanction categories.

The assessment should distinguish established harm, a substantiated risk of harm and unsupported speculation. It should consider duration, exposure, accessibility of the information, reversibility and barriers to obtaining a remedy. Evidence should make clear whether harm is widespread, concentrated in a vulnerable subgroup or particularly serious for one person.

The nature of the data and the context of its use can inform gravity under the GDPR framework, but should not become a mechanical score that replaces judgment. A transparent explanation is preferable to an undisclosed risk model or a proprietary blacklist of supposedly high-risk actors.

4 Connect sanctions to verified correction

We support distinguishing ordinary compliance from exceptional mitigating conduct, as discussed in paragraphs 77–78. An organisation should not receive automatic mitigation merely for doing what the law already required. At the same time, prompt, evidenced action that genuinely limits harm should be assessed on its merits under the applicable factors.

The guidance should identify useful evidence of remediation: when the organisation became aware, what it stopped or restricted, which recipients or systems were affected, which corrections were completed and how effectiveness was tested. A promise to improve, an unverified vendor assurance or a newly purchased audit should not carry the same weight as a demonstrated result.

For AI-related processing, deletion from one training corpus does not establish correction across model versions or generated outputs. The authority should examine the scope and limits of the action actually taken. Corrective orders should specify a measurable objective, a proportionate timetable and suitable verification while remaining grounded in the authority's legal powers.

Remediation should not create immunity from a fine, and a fine should not be treated as permission to continue unlawful processing. Where necessary and lawful, sanctions and corrective measures should work together to stop the infringement and reduce continuing harm.

5 Make enforcement reviewable and accountable

The procedural safeguards referenced in paragraph 12 should be reflected throughout the guidance. The addressee should be able to understand and challenge the material evidence, attribution, technical methods and conclusions, subject to the applicable procedural rules and legitimate protections for confidential information. A technically complex investigation must remain intelligible enough for effective review.

Independent expert assessment can be valuable when it tests a contested technical claim. Its scope, assumptions, conflicts of interest and limitations should be disclosed as appropriate. An audit should be evidence to assess, not a substitute for the authority's judgment or a presumption that all processing is compliant.

When several authorities or legal regimes address related conduct, the guidance should encourage coordination and an explicit explanation of how applicable safeguards against duplicative punishment are respected. This should not be framed as a blanket exemption from distinct lawful proceedings.

Finally, public decisions should explain the infringement and outcome while protecting complainants and third parties from unnecessary reidentification. ARGA recommends publishing meaningful reasoning and verified corrective outcomes, with appropriate redaction. Effective enforcement should improve the individual's practical position as well as deter future violations.

References

[1] EDPB Guidelines 04/2026, consultation draft, version 1.0, adopted 17 September 2026. Principal references: paragraphs 9, 12, 42–43, 48–57 and 77–78; section 5.2. Official source

[2] Regulation (EU) 2016/679, in particular Articles 58, 78 and 83 and Recital 148. Official source