Assessing remediation after financial data infringements

Comments on Guidelines 04/2026, paragraphs 73–74, 78 and 89–96

Gustavo H. R. Pessoa

Economist and professor, Fundação Getulio Vargas, São Paulo

Contribution in a personal capacity

1 November 2026

I recommend adding a short financial-data example to explain how evidence of harm mitigation should be assessed under paragraphs 73–74 and distinguished from cooperation and notification under paragraphs 89–96. This would help apply the proposed methodology consistently without creating an exemption from fines for firms that can fund an extensive response.

I am an economist and professor at Fundação Getulio Vargas, São Paulo, commenting in a personal capacity. My focus is the relationship between corrective action, the position of the affected individual and the information available for supervisory judgment. I support the Guidelines' case-by-case approach and their separation of the decision whether to impose a fine from the calculation of its amount. [1]

Evidence that shows what changed for the individual

Paragraph 74 already identifies timeliness and effectiveness as relevant to mitigation. Paragraphs 89–91 distinguish ordinary cooperation from an exceptional contribution to limiting adverse consequences. Paragraph 92 expressly recognises that financial data can cause immediate harm or distress even where it falls outside Articles 9 and 10 GDPR. These provisions provide the basis for a practical illustration, rather than a need for a new mitigation factor. [1]

Consider a hypothetical disclosure of identifiable customer transaction records through an incorrectly configured access route. The controller corrects the configuration, informs the affected individuals where legally required and offers assistance. A statement that the incident has been resolved leaves several questions unanswered. Has the exposed access route been closed and tested? Was the material copied elsewhere, so that exposure may continue? Can affected individuals obtain appropriate help without sending sensitive documents through an insecure channel? These questions concern the claimed effect of the response; they do not assume that any particular remedy can reverse an earlier disclosure.

Paragraph 78 already calls for relevant documentation, including when and how measures were taken. The financial-data example would illustrate that existing approach by linking a remedial action to the consequence it was intended to reduce. For the example above, that might include when the access route was closed, how closure was tested and which continuing risks remain. The evidence should distinguish observed results from expectations. The absence of reported fraud, on its own, cannot establish that no adverse consequences occurred: individuals may not yet know that information was disclosed, and harm can take forms other than an unauthorised payment.

The level of detail should reflect the processing and the claim being advanced. Existing incident records and a brief explanation may suffice; a universal requirement for external certification would favour organisations with greater resources and create work without necessarily improving the decision. Where a controller relies on an especially strong claim about reduced consequences, the evidence should support that claim. Supervisory authorities would retain their responsibility to assess the facts, and the controller or processor would retain applicable procedural rights.

Keep distinct grounds for mitigation clear

The same chronology should not turn one act into several automatic credits. A legally required notification, assistance in answering an authority's request and an action that reduces consequences for individuals can arise from the same incident, but they have different functions. A cross-reference between paragraphs 74, 91 and 95 could ask authorities to identify the relevant ground and explain the effect relied upon. This would preserve the Guidelines' distinction between ordinary compliance and conduct capable of receiving additional mitigating weight. [1]

A monetary payment should similarly be assessed for what it does. Returning an amount already due under a separate payment-law obligation would not by itself demonstrate exceptional cooperation with a data protection authority. Voluntary assistance may nevertheless reduce particular consequences of a data infringement. A decision should explain that connection rather than treat the amount spent as a measure of success. The proposed methodology should also remain distinct from the right to compensation under Article 82 GDPR, which concerns material or non-material damage resulting from an infringement. [2]

Prompt action should receive the weight justified by the evidence, without displacing the assessment of the infringement's gravity, duration and effects. A well-funded response cannot erase the circumstances of the original infringement or establish that it was minor merely because the organisation acted after discovery. Equally, an inability to offer an expensive assistance programme should not alone establish a failure to take effective action. The relevant question is what the measures achieved, given the circumstances and the obligations already applicable.

Suggested addition following paragraph 74

The following is proposed wording: In assessing the effectiveness of remedial measures, the supervisory authority should identify the adverse consequences which the measures address and the evidence of their effect. A chronology may help distinguish completion of an action from a demonstrated reduction in those consequences. The evidence should be proportionate to the processing and the mitigation claimed. Compliance with notification or ordinary cooperation duties should not, by itself, be treated as exceptional mitigation. Any further mitigating weight should be explained by reference to the relevant factor under Article 83(2), taking account of continuing risks and uncertainty.

This addition would make the assessment easier to explain and compare across cases. It would require neither a fixed evidence schedule nor a safe harbour. Its purpose is to help a reasoned decision show how a claimed improvement for affected individuals influenced the choice of corrective measures.

References

[1] European Data Protection Board, 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 on 17 September 2026 for public consultation Official source

[2] Regulation (EU) 2016/679, Articles 31, 33–34, 58, 82 and 83 Official source

profgustavopessoa.com/en