Contribution to the public consultation

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)

Submitted by	Thiago Francis Alves da Silva
Capacity	Independent software architect – privacy engineering, regulatory compliance infrastructure and tamper-evident audit trails
Location	Alpes-Maritimes, France
Date	28 October 2026
Previous contribution	Guidelines 02/2026 on Anonymisation (public consultation, submitted on 4 August 2026)
Publication	I consent to the publication of this contribution under my name.

Summary

Several of the factors that decide the outcome of Step 4 turn on questions of **chronology** (was a measure implemented before the investigation became known to the controller?) and of **degree** (did the measure go beyond what the GDPR requires?). The Guidelines are silent on how such facts are to be evidenced. This contribution proposes (i) an addition to paragraph 78 giving particular weight to documentation whose date and integrity can be independently verified, for instance through qualified electronic time stamps under Regulation (EU) No 910/2014 (eIDAS) or tamper-evident records, and (ii) one additional worked example for Section 5.2.13. A related clarification is suggested for paragraph 95. The proposal creates no new obligation for controllers or processors and does not weaken the presumption in favour of administrative fines.

1. Scope of this contribution

This contribution concerns Step 4 (Section 5.2), in particular paragraph 74 (Article 83(2)(c) GDPR), paragraphs 75 to 78 (Article 83(2)(d) GDPR) and paragraphs 95 and 96 (Article 83(2)(h) GDPR), with consequences for Step 5 (paragraphs 117 and 121). It is written from the perspective of a practitioner who designs the technical and organisational measures that supervisory authorities are asked to assess under these provisions.

2. Observations on the draft

2.1 Several factors depend on chronology or on degree

The Guidelines rightly set a demanding standard for mitigation, consistent with the principle that compliance with the GDPR is the norm (paragraph 88). Across Steps 3, 4 and 5, the outcome repeatedly depends on *when* a measure was taken and on *how far* it went:

- **paragraph 50** (Step 3): good faith can be invoked only in very exceptional circumstances, where the addressee took all possible and reasonable steps to avoid the infringement;
- **paragraph 74** (Article 83(2)(c)): measures spontaneously implemented prior to the investigation becoming known to the controller or processor are more likely to be considered mitigating than measures implemented after that moment;
- **paragraph 77** (Article 83(2)(d)): measures under Articles 24, 25 and 32 GDPR are mitigating only in exceptional circumstances, where the controller or processor has gone “above and beyond” its obligations;

- **paragraph 91** (Article 83(2)(f)): cooperation must go beyond what follows from applicable law or exceed what would normally be considered necessary;
- **paragraphs 95 and 96** (Article 83(2)(h)): notification of the infringement out of the controller's own motion, prior to the supervisory authority's knowledge of the case, may be mitigating;
- **paragraph 99** (Article 83(2)(i)): a reinforced commitment, such as additional measures beyond those ordered, is required for this factor to apply as mitigating;
- **paragraphs 117 and 121** (Step 5): the supervisory authority may refrain from any corrective measure where the controller took appropriate and necessary measures "as soon as it became aware" of the infringement.

Examples 12 and 13 illustrate the same logic: in Example 12 the SME amended its transparency statement before the supervisory authority initiated an investigation; in Example 13 the controller acted without waiting for the supervisory authority's decision. In both cases the decisive fact is a date.

2.2 The Guidelines do not indicate how such facts are to be evidenced

Within Step 4, paragraph 78 is the only provision dealing with the documentation provided by the controller or processor. It states that the supervisory authority should take into account any relevant documentation provided by the controller or processor, for example in the exercise of the right to be heard, and that such documentation "could provide evidence of when the measures were taken and how they were implemented". It does not indicate what makes such documentation reliable.

The Guidelines themselves recognise the problem in its negative form. In Example 4(c), where the company is unable to provide the documentation regarding the legal advice it claims to have received, the authority "cannot form a picture" of the consultation, "is therefore unable to verify" it, and the argument has no exculpatory effect. The mirror situation – documentation that exists but whose **date** and **integrity** cannot be verified – is not addressed. In practice, internal records such as policies, tickets, change logs and meeting notes can be produced or backdated after the facts, and the supervisory authority is left to weigh assertion against assertion on precisely the factors that decide the outcome of Step 4.

The Guidelines already treat technical records as part of the measures under assessment: Example 11 concerns the retention period of access logs as an element of Article 32 GDPR, Example 7 turns on the absence of systematic procedures capable of detecting an unintended configuration change, and Example 9 counts technical measures minimising the risk of re-identification among the mitigating circumstances. What is missing is only the step from "records exist" to "records can be relied upon".

2.3 Consequences

(a) Harmonisation. The Guidelines aim at a consistent and harmonised approach among supervisory authorities (paragraph 7). Without a common standard for the reliability of documentation, the same type of evidence will be weighed differently from one authority to another on the factors that are decisive in Step 4. Since the conclusions reached in Step 4 are also used when calculating the amount of the fine (paragraph 10), the divergence carries over into the application of the Calculation Guidelines.

(b) Accountability and burden of proof. The GDPR's own logic is verifiable demonstration, not assertion: Article 5(2) and Article 24 GDPR require controllers to be able to *demonstrate* compliance (paragraph 38), Recital 74 GDPR extends this to demonstrating "the effectiveness of the measures", Article 32(1)(d) GDPR requires a process for regularly testing and evaluating that effectiveness, and Article 33(5) GDPR requires breach documentation to enable the supervisory authority to *verify* compliance. The judgment cited in footnote 18 of the Guidelines (C-340/21, Natsionalna agentsia za prihodite) confirms this reading: in the context of Article 82 GDPR, the burden of proving that the technical and organisational measures are appropriate lies with the controller (operative part 3), and

an expert report cannot constitute a systematically necessary and sufficient means of proof, so that appropriateness may be established by other evidence (operative part 4). Whatever the allocation of the burden of proof in fining proceedings, the mitigating facts under Article 83(2)(c) and (d) lie within the controller's own sphere and are put forward by the controller (paragraph 78); the supervisory authority must therefore be able to assess their reliability. Paragraph 78 is the natural place to say how, and the proposal below does so in a way that remains open to any means of verification.

(c) Equal treatment. If unverifiable documentation is weighed in the same way as verifiable documentation, the factors in Article 83(2)(c), (d) and (h) favour organisations able to produce persuasive narratives over organisations with genuine technical measures. Most of the examples of minor infringements in the Guidelines concern SMEs or small organisations. Paragraph 101 recognises adherence to approved codes of conduct as a way to demonstrate compliance, but approved codes and certifications remain scarce and costly for small organisations; verifiable technical evidence offers a complementary and accessible route to the same objective.

(d) Reasoning. Supervisory authorities have the duty to state sufficient reasons for their decisions (paragraph 12). A verifiable chronology makes that duty easier to discharge, limits factual disputes during the right to be heard and reduces litigation risk on appeal.

3. Proposal

3.1 Addition to paragraph 78

The EDPB is invited to add the following text at the end of paragraph 78:

> *"Documentation whose date and integrity can be independently verified – for instance by means of qualified electronic time stamps within the meaning of Article 3(34) of Regulation (EU) No 910/2014, by tamper-evident or append-only records, or by versioned records of technical and organisational measures – should be given particular weight, notably when establishing that measures were implemented before the supervisory authority's investigation became known to the controller or processor (paragraph 74), that measures went beyond what the GDPR requires (paragraph 77), or that the controller or processor notified the infringement out of its own motion (paragraphs 95 and 96). The absence of such verifiable documentation should not, in itself, be regarded as an aggravating factor."*

Rationale. A qualified electronic time stamp enjoys a legal presumption of the accuracy of the date and time it indicates and of the integrity of the data to which they are bound (Article 41(2) of Regulation (EU) No 910/2014), and a qualified time stamp issued in one Member State is recognised in all Member States (Article 41(3)). Such time stamps are inexpensive, can be applied automatically to logs and configuration records, and are available from qualified trust service providers listed in the EU trusted lists. The reference therefore gives supervisory authorities a standard that already exists in Union law, is already harmonised, and requires no new legal instrument. The proposal is technology-neutral: qualified time stamps are given as an example because they already carry a legal presumption under Union law, but any means that allows the date and integrity of a record to be verified independently of the controller's own statements would qualify. The last sentence ensures that the clarification creates no new obligation and no additional burden for small organisations: it is a weighting rule, not a requirement.

Two limits, stated openly. First, the proposal does not interfere with national rules of evidence, to which supervisory authorities remain subject (paragraph 12): it concerns the weight that may be attached to documentation in the assessment under Article 83(2) GDPR, not its admissibility. Second, verification of date and integrity does not by itself establish that a measure was effective; it establishes when a record was made and that it has not been altered since – which is precisely the element that paragraph 78 identifies ("when the measures were taken and how they were implemented") and that is

otherwise unverifiable. The effectiveness and robustness of the measures remain to be assessed under paragraph 76.

Consequential cross-references. For consistency, paragraphs 74 and 96 could refer to paragraph 78 for the manner in which the chronology of measures and notifications may be established.

3.2 Additional worked example (Section 5.2.13)

In line with the fourteen examples in the Guidelines, the following example is proposed for Section 5.2.13 (practical examples of minor infringements). Consistent with paragraph 95, the breach notification itself is treated as neutral under Article 83(2)(h); the example rests on Article 83(2)(a), (c) and (d).

> ***Example: Verifiable evidence of pre-existing measures and of timely mitigation***
>
> *The supervisory authority found that an SME had infringed Article 32(1) GDPR following a personal data breach affecting a limited number of data subjects. The supervisory authority found that the infringement was minor within the meaning of Recital 148 GDPR and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.*
>
> *The breach resulted from a misconfiguration of a web application that exposed a customer file for a few hours. The SME notified the supervisory authority and the affected data subjects without delay. In the exercise of its right to be heard, the SME provided its access logs, a versioned record of its security measures and incident response procedure, and the configuration records showing that the customer file had been pseudonymised six months before the breach, so that the exposed data could not be directly attributed to the data subjects. Each record bore a qualified electronic time stamp. The supervisory authority was therefore able to establish, without relying on the SME's own statements, that the pseudonymisation and the incident response procedure predated the breach and that the procedure had been followed within hours of discovery. The supervisory authority considered that these measures went beyond what could be expected from an organisation of that size and that the residual risk for the data subjects was low. A somewhat aggravating factor, established from the same records, was that the misconfiguration had been flagged in the SME's own test results two weeks before the breach without being remedied in time.*

4. Related observation on paragraph 95 (Article 83(2)(h) GDPR)

Paragraph 95 treats as neutral a notification made under a specific notification obligation, such as a personal data breach notification pursuant to Article 33 GDPR. The EDPB may wish to clarify that a notification which was *not* required – for instance because the controller had documented, pursuant to Article 33(5) GDPR, that the breach was unlikely to result in a risk within the meaning of Article 33(1) GDPR, and nevertheless chose to notify – remains a notification "out of its own motion" within the meaning of paragraph 96. As drafted, paragraph 95 could be read as rendering every breach notification neutral, which would remove the incentive that Article 83(2)(h) GDPR is meant to create. The clarification would not encourage over-notification: the mitigating effect under paragraph 96 remains discretionary, and the clarification merely prevents a voluntary notification from being treated in the same way as a mandatory one. Here too, the controller's contemporaneous risk assessment is the evidence that distinguishes the two situations, and its reliability depends on the same criteria as in paragraph 78.

> *Suggested addition at the end of paragraph 95: "A notification made although it was not required under Article 33(1) GDPR, as documented pursuant to Article 33(5) GDPR, should be regarded as a notification out of the controller's own motion."*

5. Expected benefits

- The strong presumption in favour of administrative fines for non-minor infringements (paragraph 57) is untouched; the proposal only clarifies how documentation is weighed within Step 4.
- Supervisory authorities obtain a concrete and harmonised standard for the reliability of documentation, consistent with the objective of the Guidelines (paragraph 7), with the duty to state reasons (paragraph 12) and with the principle that, between equally appropriate measures, the least onerous should be chosen (paragraph 113). Since the same factors are reused when calculating the fine (paragraph 10), the standard could be mirrored in the Calculation Guidelines at their next review.
- The proposal supports dissuasiveness as described in paragraph 112, which aims to encourage compliant behaviour and to deter abstention from appropriate compliance measures: it rewards investment in verifiable accountability *before* any incident rather than narratives constructed afterwards.
- Verifiable records are credible precisely because they can also disclose facts unfavourable to the controller, as the proposed example shows. This is why they deserve particular weight, and why no controller can use them to manufacture mitigation.
- No new legal instrument and no new obligation are required: the proposal relies on Regulation (EU) No 910/2014, already in force and mutually recognised in all Member States, and expressly provides that the absence of verifiable documentation is not an aggravating factor.

I remain at the disposal of the EDPB Secretariat for any clarification on the technical aspects of this contribution.

Thiago Francis Alves da Silva
Alpes-Maritimes, France – 28 October 2026